جـــامعة محمـــــد خيضـــــر بسكـــــرة
كلية العلوم الإنسانية والاجتماعية
قسم: العلوم الإنسانية
شعبة: علم المكتبات

عنوان الأطروحة:

أثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات الجامعية بالشرق الجزائري: دراسة على عينة من المكتبات الجامعية

أطروحة مكملة لنيل شهادة دكتوراه الطور الثالث LMD في علم المكتبات
تخصص: المؤسسات الوثائقية في ظل التكنولوجيا الحديثة

إشراف الأستاذ: صغيري ميلود

إعداد الطالب: رايس عبد الوهاب

أعضاء لجنة المناقشة

الإسم واللقب	الدرجة العلمية	الجامعة	الوظيفة
كمال الصيد	أستاذ محاضر أ	جامعة بسكرة	رئيسا
ميلود صغيري	أستاذ	جامعة بسكرة	مشرفا ومقررا
وردة مصيبح	أستاذ	جامعة بسكرة	عضوا مناقشا
عبد الحميد صرايدي	أستاذ محاضر أ	جامعة بسكرة	عضوا مناقشا
سمير جزايري	أستاذ	جامعة الجزائر 02	عضوا مناقشا
عبد الهادي عبد العالي	أستاذ محاضر أ	جامعة وهران 01	عضوا مناقشا

السنة الجامعية: 2025-2026

إهداء

إلى من جعلا للنجاح معنى، وغرسا حبَّ العلم في نفسي، وسهرا على راحتي، وعجز اللسان عن تعداد فضائلهما

إلى من علّماني أن الحياة كفاح، وأن الاجتهاد طريق الوصول

إلى أبي رحمه الله رحمةً واسعة، وجعل مثواه الجنة.

وإلى أمي العزيزة حفظكِ الله سندًا لي، وبارك في عمركِ، وأدام عليكِ الصحة والعافية.

وإلى شريكة دربي ورفيقة حياتي، زوجتي الغالية، على ما بذلته من صبرٍ ودعمٍ وتشجيعٍ لا ينقطع.

وإلى فلذة كبدي وبناتي العزيزات: آلاء الرحمن، رسيل، لورين؛ أنتنَّ النور الذي يضيء دربي، والفرح الذي يمنحني القوة للاستمرار.

وإلى إخوتي وأخواتي وأبنائهم، وإلى أصدقاء الدرب القريبين والبعيدين، وإلى كل الأهل والأصدقاء.

وإلى كل من تربطني به محبةٌ ومودةٌ وصدقٌ وإخلاص.

وإلى كل طلبة العلم؛ سائلًا الله أن يجعل النجاح حليفهم، وأن يكتب لهم التوفيق والسداد.

رايس عبد الوهاب

شكروتقدير

أتقدّمُ أوّلًا بحمدِ الله تعالى وشكرِه على ما أنعم به عليّ من توفيقٍ وعونٍ وصبرٍ، حتى تمّ إنجازُ هذه الرسالة وإتمامُها.

كما يسعدني أن أتقدّم بجزيل الشكر وعظيم الامتنان إلى أستاذي المشرف الأستاذ الدكتور:"ميلود صغيري"، على إشرافه العلمي الرصين، وتوجيهاته القيّمة، وملاحظاته الدقيقة التي أسهمت في تقويم هذا العمل وإثرائه. وأثمّن عاليًا ما أبداه من دعمٍ وتشجيعٍ ومتابعةٍ مستمرة، وما تحلّى به من سعةِ صدرٍ وصبرٍ وحسنِ معاملةٍ وخلقٍ كريم، طوال مراحل إنجاز هذه الرسالة.

وأتقدّم بخالص الشكر والتقدير إلى السادة أعضاء لجنة المناقشة الموقّرين، على تفضّلهم بقبول مناقشة هذه الرسالة، وعلى ما سيقدّمونه من ملاحظاتٍ وتوجيهاتٍ علمية من شأنها الارتقاء بمستوى هذا العمل.

كما أشكر جميع الأساتذة الذين أسهموا بعلمهم وتوجيههم، وكلَّ من قدّم لي يد العون والمساعدة، سواءً بالمعلومة أو بالنصيحة أو بالدعم المعنوي، في مختلف مراحل إعداد هذه الرسالة.

ولا يفوتني أن أتوجّه بالشكر والعرفان إلى والدتي، وإلى زوجتي، وإلى بناتي: آلاء الرحمن، رسيل، لورين، على ما قدّمنه لي من دعمٍ وصبرٍ وتشجيع. كما أتقدّم بشكر خاص إلى الدكتورة:" رايس شيماء"، وإلى زملائي وزميلاتي، وكلّ من ساندني وساند مساري العلمي.

وأخيرًا، إلى كلّ من ساعدني من قريبٍ أو بعيد، أتقدّم بخالص الشكر وعظيم الامتنان.

قـائمة المـختصـرات

الإختصار	المصطلح باللغة الإنجليزية	المصطلح بالعربية	الصفحة
ARMA	Association of Records Managers and Administrators	جمعية إدارة السجلات والمعلومات	48–41
CMMI	Capability Maturity Model Integration	نموذج نضج القدرات المتكامل	130
COBIT	Control Objectives for Information and Related Technologies	أهداف التحكم في المعلومات والتكنولوجيا ذات الصلة	130
COSO	Committee of Sponsoring Organizations of the Treadway Commission	لجنة المنظمات الراعية للجنة تريدوي	130
DDOS	Distributed Denial of Service	الهجمات الموسعة لحجب الخدمة	87
DSA	Digital Services Act	قانون الخدمات الرقمية	56
GDPR	General Data Protection Regulation	اللائحة العامة لحماية البيانات	62
HTTPS	HyperText Transfer Protocol Secure	برتوكول نقل النص التشعبي الامن	118
IAM	Identity and Access Management	أنظمة إدارة الهوية والوصول	150
IDS	Intrusion Detection System	نظام كشف التسلل	90
IEC	International Electrotechnical Commission	اللجنة الكهروتقنية الدولية	134
IG	Information Governance	حوكمة المعلومات	41
ISACA	Information Systems Audit and Control Association	جمعية التدقيق والرقابة على أنظمة المعلومات	135
ISMS	Information Security Management System	نظام إدارة أمن المعلومات	108
ISO	International Organization for Standardization	منظمة التقييس العالمية	43– 56–51
ITG	Information Technology Governance	حوكمة تكنولوجيا المعلومات	43
ITIL	Information Technology Infrastructure Library	مكتب البنية التحتية لتكنولوجيا المعلومات	130
KPIS	Key Performance Indicators	مؤشرات الأداء الرئيسية	280
LTDB	Long–Term Data Backup	النسخ الإحتياطي للبيانات طويل الأمد	111
MFA	Multi-Factor Authentication	المصادقة متعددة العوامل	48
MFA	Multi–Factor Authentication	المصادقة متعددة العوامل	67
NCA	National Cybersecurity Authority	الهيئة الوطنية للأمن السيبراني	85
OECD	Organisation for Economic Co-operation and Development	منظمة التعاون الاقتصادي والتنمية	39

قـائمة المـختصـرات

RM	Risk Management	إدارة المخاطر	78
SOPS	Standard Operating Procedures	إجراءات التشغيل القياسية	279
SSL	Secure Sockets Layer	طبقة المقابس الامنة	118
SSO	Single Sign–On	تسجيل الدخول الأحادي	152
UNDP	United Nations Development Programme	البرنامج الإنمائي للأمم المتحدة	40

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

قـائمة المحـتويات

مقدمة

مـقدمـة

إنتقال المكتبات الجامعية من الإدارة التقليدية إلى الإدارة الإلكترونية وتطور خدمات المعلومات وإستخدام قواعد البيانات في الحفظ وتخزين المعلومات والبيانات يعكس التحول الإستراتيجي للمكتبات، نحو توظيف التكنولوجيا الجديدة في المهنة المكتبية كمحاولة لإمتصاص الكثير من التعقيدات في الإجراءات المكتبية، ومن أهم إنجازات هذا التحول الرقمنة، هذا الأمر الذي أضحى حتمية وليس خيار في وقتنا الراهن نظرا لحاجة مؤسسات المعلومات إلى عصرنة الوظائف والخدمات المكتبية بما يتوافق مع متطلبات العصر الحالي. ولأن التحول الرقمي كان له إنعكاسات في العديد من الممارسات والأدوار الإدارية والفنية والتنظيمية؛ ظهرت مجموعة من البيانات والمعلومات مرتبطة بالمستخدمين والمستفيدين والمجموعات المكتبية مخزنة في خوادم، وخدمات معلومات متاحة على شبكة الأنترنت مثل: المكتبات الرقمية وفهارس البحث على الخط وغيرها.

نتيجة الإنفجار المعرفي والتحولات الرقمية المتسارعة ومع تزايد الإعتماد على البيانات لم تعد المكتبات مجرد مؤسسات حفظ وتنظيم مصادر المعلومات بل أصبحت مرافق فاعلة في إدارة المعرفة ودعم إتخاذ القرار، هذا الواقع فرض تحديات جديدة تتعلق بجودة المعلومات وأمنها وحمايتها. الأمر الذي جعل توجه مؤسسات المعلومات والمكتبات الجامعية خاصة نحو حوكمة المعلومات ضرورة إستراتيجية لضمان حماية الموارد الرقمية وتحسين خدمات المعلومات وتحقيق الإنفتاح الأكاديمي.

كما أن هذا التوجه جاء نتيجة الحاجة للإمتثال للمعايير الدولية وتزايد مخاطر الأمن السيبرانية التي تلمس الأنظمة الآلية المخصصة في إدارة وتسيير المكتبات وقواعد البيانات والخوادم والمستودعات المؤسساتيةوالتي تعد مركز حفظ البيانات في المؤسسة. وتطبيق حوكمة المعلومات أحد الحلول التي تحقق ضمان إستدامة وحماية الموارد الرقمية للمكتبات وإستمرارية خدماتها الرقمية بما يسهم في دعم إتخاذ القرار بالإعتماد على بيانات موثوقة ومؤمنة.

وبما أن الخدمات الحديثة للمكتبات الجامعية تستخدم أنظمة آلية في أرشفة البيانات وإتاحتها في شكل معلومات متاحة على شبكة الانترنت، فإن ضمان حماية وخصوصية البيانات والمعلومات أحد أبرز التحديات التي تواجه مؤسسات المعلومات في ظل التجاوزات والإختراقات التي يشهدها الفضاء السيبراني. وهذا لن يتأتى إلا من خلال وضع مجموعة من السياسات والمعايير والأدوار والإجراءات التي تضمن الإستخدام الأمثل للمعلومات إنتاجا وتخزينا ومعالجة وإسترجاعا.

حوكمة المعلومات في المكتبات الجامعية الجزائرية لم تعد مجرد إجراء إداري بل إطار إستراتيجي يربط بين المعرفة والتكنولوجيا والقوانين لضمان تقديم خدمات معلومات عالية الجودة، وخصوصا في الفضاء السيبراني الذي يجمع الأنظمة وشبكة الانترنت والتفاعلات الرقمية.

ولمعالجة موضوع الدراسة تم تقسيم البحث إلى فصول رئيسية تتخللها عدة مباحث ومطالب، تتمثل في:

الفصل الأول: يمثل القاعدة المنهجية والبنائية للظاهرة المدروسة حيث ينقسم الفصل إلى شقين أساسين مرتبطان بعضه البعض والمتمثل في : أساسيات الدراسة وإجراءات الدراسة الميدانية؛ تعنى أساسيات الدراسة في تحديد وضبط إشكالية وأسئلة الدراسة المبحوثة وفرضيات الدراسة والوقوف على أهمية الدراسة والأهداف المراد بلوغها وأيضا المنهج المعتمد في معالجة الموضوع والدراسات السابقة ذات الصلة بالبحث وضبط المفاهيم ومصطلحات الدراسة، أما الشق الإجرائي للدراسة يتضمن مجالات الدراسة؛ المجال الجغرافي والزمني والبشري. كما حددت الدراسة مجتمع وعينة الدراسة وأدوات مجتمع البيانات.

الفصل الثاني: يناقش الفصل الجذور النظرية والمفاهيمية لحوكمة المعلومات والمفاهيم المرتبطة به ممثلة في: حوكمة تكنولوجيا المعلومات وحوكمة البيانات وحوكمة المؤسسات وحوكمة إدارة السجلات وحوكمة نظم المعلومات، كما يسلط الضوء على دوافع ومبررات توجه حوكمة المعلومات. إضافة إلى ذلك عرجت الدراسة للوقوف على الأدوار المحورية لحوكمة المعلومات على المستوى التنظيمي والقانوني في المؤسسات سواء كانت ربحية أو مؤسسات غير ربحية، وأهدافها. وفي الأخير عرضت الدراسة مبادئ وأبعاد حوكمة المعلومات.

الفصل الثالث: يناقش الإطار المفاهيمي للأمن السيبراني وأهميته في المكتبات الجامعية، كما أظهرت الدراسة الأهداف المحورية للأمن السيبراني وتأثيره على الخدمات المكتبية الرقمية. كما يوضح الفصل أنواع مخاطر الأمن السيبراني في المكتبات الجامعية من الناحية التقنية وأيضا الممارسات البشرية؛ والتي تعد أحد أبرز التهديدات التي ترافق أنظمة المكتبات وقواعد البيانات خصوصا الخدمات الإلكترونية، كما أظهرت الدراسة إستراتيجية إدارة مخاطر الأمن السيبراني في المكتبات الجامعية، وتقنيات الحماية والتحديات التي تواجه المكتبات الجامعية كمؤسسة معلومات لتعزيز أمنها وسلامتها.

الفصل الرابع: يعالج دور حوكمة المعلومات على مخاطر الأمن السيبراني في المكتبات الجامعية وذلك من خلال إبراز مكانة حوكمة المعلومات والأمن السيبراني في المكتبات وفوائد حوكمة المعلومات على مخاطر الأمن السيبراني، كما عرجت الدراسة إلى تسليط الضوء على أطر وسياسة حوكمة المعلومات وأثر تطبيقها لتعزيز وتحقيق الأمن في الأنظمة والمواقع وقواعد البيانات بما يدعم الحفاظ على السرية وخصوصية البيانات والمعلومات، وأيضا التحديات والفرص المتوقعة منه.

الفصل الخامس: يعالج الفصل المكتبات الجامعية الجزائرية؛ تعريفها ودورها في مؤسسات التعليم العالي والبحث العلمي والخدمات التي تقدمها للمجتمع الأكاديمي. كما أظهرت الدراسة مخطط الدراسة الإستطلاعية المنجزة، بهدف تحديد ملامح البحث العلمي وضبط حدوده وأدواته، والوقوف على مراحل الدراسة الإستطلاعية ومخرجاتها.

الفصل السادس: يناقش هذا الفصل مستوى وعي أخصائي المعلومات بالمكتبات المركزية بجامعات الشرق الجزائري بحوكمة المعلومات لمخاطر الأمن السيبراني ومستوياته، وأيضا أثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات المركزية عينة الدراسة، كما حاولت الدراسة تسليط الضوء على الفروقات في مستوى مخاطر الأمن السيبراني بما يعزز السوسيوديموغرافية لأخصائي المعلومات بالمكتبات محل الدراسة، قام الباحث بإختبار الفرضيات وتحليلها وفق معادلات إحصائية وتفسيرها وعرض النتائج العامة وتقديم مجموعة من التوصيات.

الفصل الأول:

الإطار المنهجي وإجراءات الدراسة

تمهيد

البحث العلمي مبني بدرجة كبيرة في تحديد الإطار المنهجي المناسب للدراسة بهدف الوصول إلى نتائج منطقية، الأمر الذي يتطلب وضع فرضيات علمية مقترحة للإجابة عن تساؤلات الدراسة، وتحديد أهميتها وأهدافها المرجوة وأيضا العوامل الأساسية لإختيار الموضوع. كما تم إختيار الأدبيات التي لها صلة بموضوع البحث ووضع المنهج العلمي المناسب، كما يرتكز البحث على تحديد إجراءات الدراسة الميدانية من خلال العناصر التالية: مجتمع وعينة الدراسة ومجالات الدراسة بحدودها الجغرافية والزمنية والبشرية، وأدوات جمع البيانات المعتمدة للوصول إلى حقائق علمية وتفسيرها وتحديد المفاهيم الدالة عن الموضوع.

1.1 أساسيات الدراسة

تتحدد أساسيات الدراسة في الإطار المنهجي المعتمد في دراسة الموضوع ومتغيراته الأساسية.

1.1.1 إشكالية الدراسة

أمام التطورات المتسارعة وبالخصوص المتعلقة بتكنولوجيا المعلومات والإتصال؛ وتوجه المكتبات الجامعية نحو التحول الرقمي في أنشطتها وعملياتها الفنية والإدارية، إزدادت أهمية المعلومات وإرتفعت قيمتها نظرا لأهميتها الكبيرة في المؤسسة. والمعلومات تعد القاعدة المعرفية التي تستند عليها في صياغة القرارات وإدارة العمليات في المحيط الداخلي والخارجي، الأمر الذي دفع بالمكتبات الجامعية نحو الاعتماد على أنظمة المعلومات للتحكم والسيطرة على هذا المورد المهم لتحقيق الجودة والتميز في الأداء.

إنفتاح المكتبات الجامعية والمكتبات الجامعية الجزائرية على نحو خاص في البيئة الرقمية نتيجة التحول الرقمي والحوسبة بإستخدام نظم المعلومات في إدارة وتسيير الوظائف والخدمات المكتبية، رافقه تحديات كبيرة ناتجة عن بيئة الفضاء الرقمي وخصوصيته؛ تتميز هذه البيئة بالتغير الديناميكي وتعدد وتنوع أدواتها وتقنياتها المستخدمة، بالإضافة إلى عدم قدرة المكتبات على السيطرة على المتغيرات التقنية التي تمثل خطروتحدي لهذه المكتبات، فهي تهددها في سلامة وسرية وتوافر معلوماتها في الفضاء السيبراني مما يؤثر على رسالة ورؤية وأهداف المكتبة الجامعية ثم في بقائها وإستمرارها و قدرتها على منافسة المكتبات الجامعية الأخرى.

هذه المعطيات والتغيرات المستمرة إستوجب على المكتبات إستخدام أساليب جديدة للتأقلم مع هذه المتغيرات، من خلال زيادة قدرتها على توقع المخاطر والجاهزية لمواجهتها بهدف التقليل من الأضرار عند حدوثها. عن طريق وضع إستراتجيات وأسس وأطر تنظيمية وتقنية وفنية لإدارة وضبط المعلومات في المكتبات محاولة لإحتواء الضرر قبل وأثناء وبعد الأزمة.

في خضم ذلك، حوكمة المعلومات وتحليل مخاطر الأمن السيبراني تسهم في جودة المعلومات وإتخاذ القرارات وتنفيذ السياسات والإجراءات المتعلقة بالمكتبة والحد من المخاطر المحتملة، مما يجعل تطبيق المكتبات الجامعية لحوكمة المعلومات كأسلوب وآلية جديدة للحد من المخاطر الأمن السيبراني وسط التغيرات التقنية المتسارعة أمرا لا مفر منه؛ فهي تساعد على خلق مناخ جيد لأخصائي المعلومات للتعامل مع المخاطر السيبرانية من خلال القدرة

على الإستشراف والرؤية المستقبلية ؛ والإبداع في حل المشكلات وفهم العلاقات المتداخلة ،وفهم البيئة الداخلية والخارجية للمكتبات الجامعية.

إستنادا لما سبق، فقد ركزت الدراسة على معالجة حوكمة المعلومات وأثرها على مخاطر الأمن السيبراني في المكتبات الجامعية بالشرق الجزائري من خلال قياس مستوى وعي أخصائي المعلومات وإلمامهم بالموضوع؛ بإستخدام مبادئ حوكمة المعلومات ومبادئ مخاطر الأمن السيبراني لقياس الأثر. ومن هذا المنطلق، جاء السؤال الرئيسي للدراسة على النحو الآتي:

ما أثر حوكمة المعلومات على مخاطر الأمن السيبراني في المكتبات المركزية بجامعات الشرق الجزائري؟

2.1.1 أسئلة الدراسة

تتفرع الإشكالية العامة للدراسة من مجموعة من الأسئلة الفرعية تمثل في مايلي:

1. ما مستوى وعي أخصاصي المعلومات محل الدراسة بحوكمة المعلومات لمخاطر الأمن السيبراني؟
2. ما مستوى حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري؟
3. ما مستوى مخاطر الأمن السيبيراني بالمكتبات المركزية لجامعات الشرق الجزائري؟
4. ما أثر تطبيق حوكمة المعلومات على مخاطر الأمن السيبيراني بالمكتبات المركزية لجامعات الشرق الجزائري؟
5. هل توجد فروق في مستوى مخاطر الأمن السيبراني تعزى السوسيوديمغرافية لأخصائي المعلومات بالمكتبات محل الدراسة؟

3.1.1فرضيات الدراسة

تعتبر الفرضيات العلمية أكثر صور التعبير عن مشكلة الدراسة دقة ووضوحا، ومن خلال ماسبق حاول الباحث إختيار الفرضيات التالية لمعالجة إشكالية الدراسة:

1.3.1.1 الفرضية الأساسية

حوكمة المعلومات لها أثر إيجابي في التقليل من مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري.

2.3.1.1 الفرضيات الفرعية للدراسة:

قسمت الفرضية الأساسية إلى مجموعة من الفرضيات الفرعية، وهي كالآتي:

الفرضية الأولى:

- مستوى وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبيراني بالمكتبات المركزية لجامعات الشرق الجزائري منخفض.

الفرضية الثانية:

- مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري متوسط

الفرضية الثالثة:

- مستوى مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي.

الفرضية الرابعة:

- أثر تطبيق حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي.

الفرضية الخامسة:

- لا توجد فروق ذات دلالة إحصائية في مستوى مخاطر الأمن السيبراني تعزى السوسيوديمغرافية لأخصائي المعلومات بالمكتبات محل الدراسة.

4.1.1 أهمية الدراسة

المكتبات الجامعية مركز للمعرفة ودعامة أساسية في التعليم والبحث من خلال توفير الوصول إلى مجموعة واسعة من مصادر المعلومات. وهي ضرورية لتسهيل النجاح الأكاديمي وتعزيز الابتكار بين الطلاب وأعضاء هيئة التدريس والباحثين. وعليه فإن الاعتماد المتزايد على الموارد الرقمية ووزيادة البيانات جعل المكتبات عرضة لتهديدات الأمن السيبراني. ومن هذا المنطلق تظهر أهمية الدراسة من أهمية حوكمة المعلومات في المكتبات الجامعية حيث تتضمن حوكمة المعلومات الفعالة تنفيذ السياسات والإجراءات والتقنيات لإدارة وحماية أصول المعلومات. وفي سياق المكتبات الجامعية، تساعد في الحماية من الوصول غير المصرح به وإنتهاكات البيانات والتهديدات السيبرانية من خلال ضمان سلامة المعلومات وسريتها وتوافرها.كما تبرز أهمية الدراسة في الإشارة إلى دور حوكمة المعلومات في تقليل مخاطر الأمن السيبراني في المكتبات الجامعية بناء على الأطر والمعايير محددة

بهدف خلق بيئة آمنة للأنشطة الأكاديمية. ذلك أن دور حوكمة المعلومات لا يحمي البيانات القيمة الموجودة داخل هذه المكتبات فحسب بل يعزز أيضًا قدرتها على خدمة المجتمع الأكاديمي بكفاءة وأمان.

5.1.1 أسباب إختيار الموضوع:

إختيار موضوع حوكمة المعلومات وأثرها على مخاطر الأمن السيبراني في المكتبات الجامعية ينبع من عدة أسباب رئيسية وهي كمايلي:

- حداثة موضوع حوكمة المعلومات في المكتبات الجامعية.
- المعارف والمكتسبات السابقة للباحث حول موضوع حوكمة المعلومات ومخاطر الأمن السيبراني في المكتبات السيبراني.
- الخبرة المهنية للباحث في مجال الأمن السيبراني والتقنية في المكتبات الجامعية.
- الإهتمام الشخصي للباحث في معالجة حوكمة المعلومات في بيئة المكتبات .

6.1.1 أهداف الدراسة:

نسعى من خلال دراستنا؛ تحقيق جملة من الأهداف وهي كمايلي:

- التعرف على حوكمة المعلومات ومبادئها ومجالات تأثيرها على مخاطر الأمن السيبراني بالمكتبات الجامعية.
- تعميق المعرفة العلمية في مجال حوكمة المعلومات ومخاطر الأمن السيبراني.
- معرفة مستوى وعي أخصائي المعلومات بالمكتبات محل الدراسة بحوكمة المعلومات لإدارة مخاطرالأمنالسيبراني.
- معرفة مستوى حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري.
- التعرف على مستوى مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري.
- قياس أثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري
- معرفة الفروق في مستوى مخاطر الأمن السيبراني تعزى السوسيوديمغرافية لأخصائي المعلومات بالمكتبات محل الدراسة.
- التوصل إلى نتائج يمكن على ضوئها تقديم اقتراحات للقائمين على المكتبات الجامعية تساعد في تجسيد برامج حوكمة المعلومات في الواقع للارتقاء بجودة آداء المكتبات الجامعية لمستوى طموحات الاطراف ذات المصلحة الداخلية والخارجية.

7.1.1 منهج الدراسة

يعد المنهج أحد أساسيات البحث العلمي الذي يتبعه الباحث في دراسته للوصول إلى الأهداف المرجوة وتحقيق نتائج منطقية، وبالنظر إلى موضوع البحث إرتأينا إلى إعتماد المنهج الوصفي، يسمح بالبحث عن أوصاف دقيقة للظاهرة المراد دراستها، عن طريق مجموعة من الأسئلة التي يتم الإجابة عليها من خلال جمع

الحقائق والبيانات الكمية والكيفية عن الظاهرة المحددة، ومحاولة تحليل البيانات وتفسيرها بهدف إستخراج الإستنتاجات ذات الدلالة وتعميم النتائج[1].

كما يهتم المنهج الوصفي برصد ومتابعة الظاهرة التي تم معالجتها كما هي من حيث خصائصها وأشكالها والعوامل المؤثرة في جميع جوانب الأبعاد المتعلقة بها، حيث تم الوصول إلى النتائج التي تساعد في فهم الحاضر والتنبؤ بالمستقبل[2].

8.1.1 الدراسات السابقة

تم الاعتمادفي بناء الدراسات السابقة على مجموعة من الدراسات لتحديد نقاط التوافق والإختلاف في الدراسات العلمية وموضوع البحث والوقوف على القيمة المضافة ونتائج ومقترحات الدراسة. شملت دراسات عربية وأجنبية يتحدد مجالها الموضوعي في حوكمة المعلومات، ومخاطر الأمن السيبيراني. تم تصنيف الدراسة حسب تسلسلها الزمني من الأحدث إلى الأقدم وعرضها كالآتي:

1.8.1.1 الدراسات العربية

الدراسة الأولى: دور تطبيقات الحوكمة في تحقيق الجودة الشاملة بالمكتبات الجامعية: دراسة ميدانية بالمكتبات الجامعية لجامعات الشرق الجزائري. زيادي كريمة، 2024[3].

الدراسة أطروحة دكتوراه؛ هدفت الدراسة إلى إبراز دور تطبيقات الحوكمة في تحقيق الجودة الشاملة في المكتبات الجامعية، إعتمدت الباحثة على المنهج الوصفي، وأدوات جمع البيانات؛ الملاحظة وإستمارة الاستبيان. طبقت على جميع المكتبات المركزية المتواجدة على مستوى جامعات الشرق الجزائري. أظهرت نتائج الدراسة أن تطبيق الحوكمة له دورجد فعال في سبيل بلوغ الجودة الشاملة ويتجسد في تعزيز الشفافية والمساءلة وخلق روح التعاون بين الأفراد، والتي ترتبط بشكل مباشر بالتخطيط والتنظيم والرقابة وكذا تقييم الآداء بالمكتبة مما يزيد من نسبة الآداء الوظيفي ويحسن من الفاعلية التنظيمية وخلق ميزة تنافسية، مما يساعد وبشكل كبير في تحقيق الجودة الشاملة بالمكتبات الجامعية.

---

[1]. دشلي،كمال .**منهجية البحث العلمي** .حماة: مديرية الكتب والمطبوعات الجامعية،2016. ص61.

[2]. دشلي،كمال. **المرجع السابق**.ص61.

[3].زيادي، كريمة. **دور تطبيقات الحوكمة في تحقيق الجودة الشاملة بالمكتبات الجامعية: دراسة ميدانية بالمكتبات الجامعية لجامعات الشرق الجزائري**. أطروحة دكتوراه تخصص: إدارة وتسيير المكتبات ومراكز التوثيق. جامعة تبسة، 2024

وفي ضوء ما سبق، خلصت الدراسة إلى ضرورة تعيين مسؤولين أكفاء وتعزيز المشاركة الاجتماعية من طرف مسؤولي المكتبات الجامعية، تحديد خطط وإستراتجيات واضحة بأهداف وتوجه المكتبات. كما أكدت الدراسة على ضرورة تطبيق مبدأ الشفافية والمسائلة في المكتبات.

تتقاطع الدراسة مع موضوع الدراسة في المجال الجغرافي، كما تناقش موضوع الحوكمة في مجال الجودة الشاملة. تم الإعتماد على الدراسة في الجانب النظري والمتمحور في مبادئ الحوكمة.

الدراسة الثانية: نحو حوكمة نظم المعلومات في مؤسسات التعليم العالي: دراسة حالة عينة من مؤسسات التعليم العالي. مسوس كمال، 2018[1]

الدراسة أطروحة دكتوراه، عرضت وضعية نظم المعلومات الحديثة في مؤسسات التعليم العالي الجزائرية وتوجهاتها نحو إدارة وحوكمة نظم المعلومات بواقع مؤسسات التعليم العالي العمومية والخاصة المتقدمة في هذا المجال، شملت عينة مؤسستين من مؤسسات التعليم العاليممثلة في جامعة العلوم والتكنولوجيا هواري بومدين وجامعة الجزائر 3 ابراهيم سلطان شيبوط. هدفت الدراسة إلى الوقوف على واقع نظم المعلومات الحديثة والجوانب المتعلقة وإدارتها وحوكمتها في الجامعات عينة الدراسة، وإبراز أهمية نظم المعلومات الحديثة التي تلبي إحتياجات أصحاب المصالح في المحيط الداخلي والخارجي وتقديم أهم الحلول التي تضمن سرية وسلامة وتوافر المعلومات. وقدمت الدراسة نماذج وتجارب حوكمة نظم المعلومات في مؤسسات التعليم العالي.

خلصت الدراسة إلى أن واقع نظم المعلومات الحديثة وفق المحاور التي تم معالجتها ضعيفة على مستوى المصالح ومديريات الجامعات ودون المتوسط على مستوى الموارد البشرية وأمن المعلومات، فواقع نظم المعلومات الحديثة لا يتماشى مع الإتجاهات الحديثة في إدارة وتسيير النظم. كما أظهرت الدراسة أن واقع نظم المعلومات بجامعة العلوم والتكنولوجيا هواري بومدين وجامعة الجزائر 3 لا يساعد على التوجه نحو حوكمة نظم معلومات. أوصت الدراسة ضرورة مراجعة السياسات والإستراتيجيات المتعلقة بالمؤسسات الجامعية ونظم المعلومات الحديثة، وتشكيل لجنة دائمة خاصة بحوكمة نظم المعلومات.

تم الإستفادة من الدراسة في الجانب النظري من خلال معرفة طبيعة وخصوصية نظم المعلومات في الجامعات الجزائرية عينة الدراسة وواقع تطبيق حوكمة النظم خصوصا أن واقع نظم المعلومات وسياساته تتقاطع مع نظم إدارة وتسيير المكتبات، وأيضا الوقوف على المقاربات واطر حوكمة نظم المعلومات في المؤسسة.

---

[1]. مسوس، كمال. **نحو حوكمة نظم المعلومات في مؤسسات التعليم العالي: دراسة حالة عينة من مؤسسات التعليم العالي.** أطروحة دكتوراه. تخصص: تسيير عمومي. جامعة الجزائر 3، 2018.

2.8.1.1 الدراسات الأجنبية

الدراسة الأولى:

Tonia San Nicolas-Rocca. Information Security in Libraries: Examining the Effects of Knowledge Transfer, 2019[1]

هدفت الورقة العلميةإلى تقيم أثر نقل المعرفة كوسيلة لتعزيز أمن المعلومات داخل المكتبات، تم إجراء البحث بناء على دورة للأمن السيبراني عبر الأنترنت مقدمة في إحدى الجامعات الأمريكية ، تشير نتائج أداة المسح المستخدمة في جمع البيانات:أن نقل المعرفة من خلال تعليم الأمن السيبراني يمكن أن يؤدي إلى إستخدام المعرفة وعلى وجه التحديد قد يؤثر نقل المعرفة من خلال تعليم الأمن السيبراني على موظفي المكتبة للاستفادة من المعرفة المكتسبة من خلال المناقشات حول المساءلة والمسؤولية وزيادة الوعي بحماية المعلومات الخاصة بالمستفيد. وتشير نتائج الدراسة أن نقل نقل المعرفة له تأثير إيجابي على ممارسات أمن المعلومات وإدارة المخاطر لدى موظفي المكتبات.

ساهمت الدراسة في التعمق حول موضوع الأمن السيبيراني وجوانب تطبيقه في المكتبات في الجانب الميداني وضبط مؤشرات أداة جمع البيانات.

الدراسة الثانية:

Anderfuhren, Sandrine .Romagnoli, Patrizia.La maturité de la gouvernance de l’information dans les administrations publiques européennes : la perception de la gouvernance de l’information dans l’administration publique genevoise, 2018[2]

تناولت مذكرة ماجستير؛ حوكمة المعلومات في الإدارات العامة جنيف، ومدى تطبيق المتخصصين في إدارة المعلومات والأرشفة مبادئ حوكمة المعلومات. كما تسلط الضوء على مقاربات وأبعاد حوكمة المعلومات بإعتبارها

---

[1]. Tonia San Nicolas-Rocca. **Information Security in Libraries**: **Examining the Effects of Knowledge Transfer**. Information Technology and Libraries, Vol.38, N.02, 2019

[2]. Anderfuhren, Sandrine.Romagnoli, Patrizia.**La maturité de la gouvernance de l’information dans les administrations publiques européennes** : **la perception de la gouvernance de l’information dans l’administration publique genevoise**. Mémoire de recherche. Haute École de Gestion de Genève, 2018

مرجعية أساسية لإدارة المخاطر. هدفت الدراسة إلى تقديم تصور لممارسات تطبيق حوكمة المعلومات في المؤسسة بإستخدام نموذج نضج حوكمة المعلوماتARMA لتقييم ممارساتها وتحسينها.

إعتمد الباحث على الدراسة في تحديد وضبط مبادئ حوكمة المعلومات وتوظيفها في تحديد مؤشرات أداة البحث.

9.1.1 مفاهيم ومصطلحات الدراسة

تتحدد المفاهيم الأساسية للدراسة وفق المنظور الإجرائي للباحث في مايلي:

1. المكتبات الجامعية

المكتبة الجامعية هي مؤسسة علمية، ثقافية، تربوية وإجتماعية تابعة للجامعة، تقدم مجموعة شاملة من موارد المعرفية والمعلوماتية (كتب، مجلات، ومقالات علمية،ورسائل وأطروحات جامعية،موارد رقمية) لمستفيديها من خلال مجموعة من الخدمات، توفر الموارد المعرفية فرصة الوصول إلى المعلومات الأكاديمية والعلمية في مختلف التخصصات العلميةبهدف دعم وتعزيز البحث والدراسة والإبتكار.

2. حوكمة المعلومات:

هي إطار عمل يشمل على المعايير والعمليات والأدوار والمقاييس التي تجعل المؤسسات والأفراد مسؤولين عن توليد المعلومات وتنظيمها وتأمينها وحفظها واستخدامها والتخلص منها بطريق تتناسب مع أهداف المؤسسة ورؤيتها.كما تستند حوكمة المعلومات على إستراتيجية واضحة وموثقة في إدارة المعلومات من أجل حفظ التكاليف وتقليل المخاطر وضمان الإمتثال للمعايير القانونية والتنظيمية وحوكمة المؤسسات.

3. الأمن السيبراني:

مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى حماية الأنظمة المعلوماتية وشبكات الإتثال والبيانات من الهجمات الإلكترونية والإختراقات لضمتن سرية وسلامة البيانات.

4. مخاطر الأمن السيبراني:

في مجموعة من التهديدات التي تستهدف أنظمة المعلومات؛ البرامج والشبكات وترتبط هذه التهديدات بالبرامج الخبيثة والإختراقات.

2.1 إجراءات الدراسة الميدانية

توضح إجراءات الدراسة الميدانية محددات موضوع البحث، تشمل حدود الدراسة، ومجتمع وعينة الدراسة وأيضا الأداة المستخدمة في جمع البيانات الدراسة.

1.2.1 مجالات الدراسة

تنقسم مجالات الدراسة إل ثلاثة (03) حدود أساسية توضح معالم موضوع البحث، وهي كالتي:

1.1.2.1 المجال الجغرافي :

يتمثل النطاق الجغرافي للدراسة في جميع المكتبات المركزية التابعة لجامعات الشرق الجزائري وفق توزيع المؤسسات الجامعية بموقع وزارة التعليم العالي والبحث العلمي.

2.1.2.1 المجال الزمني:

تشمل الحدود الزمنية على مجموعة من المراحل، بداية من الحصول على الموافقة حول موضوع البحث، ثم الإطلاع على الأدبيات وجمع مصادر المعلومات المتعلقة بمجال الدراسة ومتغيراتها الأساسية؛ والممتدة من 2023 إلى 2024، والشروع في هيكلة وبناء إطار الدراسة وبناء المحتوى من الناحية النظري والميدانية، وفي الأخير مرحلة جمع وتحليل معطيات الدراسة الممتدة من شهر فيفري 2025 إل غاية 2026.

3.1.2.1المجال البشري:

الأفراد المبحوثين يشمل جميع الموظفين الإداريين والتقنيين العاملين بالمكتبات المركزية لجامعات الشرق الجزائري، متخصص في علم المكتبات والتوثيق. تشمل الدراسة 148مكتبي موزعين في الأسلاك التالية:

- عون تقني بالمكتبات الجامعية
- مساعد بالمكتبات الجامعية
- ملحق بالمكتبات الجامعية من المستوى الاول والثاني
- محافظ بالمكتبات ورئيسي محافظي المكتبات الجامعية.

2.2.1 مجتمع وعينة الدراسة

يتحدد مجتمع الدراسة في مجموعة الوحدات ووالمفردات المعرفة بصورة واضحة لموضوع البحث، ويتمثل مجتمع الدراسة في جميع الموظفين العاملين بالمكتبات المركزية لجامعات الشرق الجزائري، ومن أجل معرفة الجامعات المعنية

تم الاعتماد على موقع الندوة الجهوية لجامعات الشرق الجزائري[1]. تم إحصاء **22جامعة**؛ بما يعادل **22 مكتبة مركزية**، بلغ عدد الموظفين بالمكتبات المركزية ب: **429 موظف**. والجدول الموالي يوضح توزيع المكتبات المركزية لجامعات الشرق الجزائري وعدد الموظفين بالمكتبات المركزية بشكل رسمي في الجامعة.

الجدول رقم(01): مجتمع الدراسة

الرقم	الجامعة	عدد الموظفين الاجمالي
01	المكتبة المركزية لجامعة الشهيد العربي التبسي–تبسة	13
02	المكتبة المركزية لجامعة باتنة1–الحاج لخضر	29
03	المكتبة المركزية لجامعة باتنة2– مصطفى بن بولعيد	16
04	المكتبة المركزية لجامعة فرحات عباس –سطيف1	34
05	المكتبة المركزية لجامعة الهضاب –سطيف2	14
06	المكتبة المركزية لجامعة الامير عبد القادر –قسنطينة1	32
07	المكتبة المركزية لجامعة محمد ميرة –جيجل	29
08	المكتبة المركزية لجامعة الاخوة منتوري –قسنطينة1	34
09	المكتبة المركزية لجامعة الشاذلي بن جديد –الطارف	11
10	المكتبة المركزية لجامعة عباس لغرور – خنشلة	20
11	المكتبة المركزية لجامعة ام البواقي	42
12	المكتبة المركزية لجامعة الوادي	10
13	المكتبة المركزية لجامعة سوق هراس	15
14	المكتبة المركزية لجامعة عنابة	33
15	المكتبة المركزية لجامعة سكيكدة	18
16	المكتبة المركزية لجامعة 8 ماي1945 –قالمة	13
17	المكتبة المركزية لجامعة بسكرة(مكتبة القطب الجديد– المجمع القديم)	16
18	المكتبة المركزية لجامعة المسيلة	12
19	المكتبة المركزية لجامعة ورقلة	11
20	المكتبة المركزية لجامعة برج بوعريريج	9

[1]. الندوة الجهوية للشرق الجزائري. تاريخ الإطلاع: 25-12-2023، على الساعة: 14:45. متاح على الرابط: /https://www.univ-constantine2.dz/cruest

21	المكتبة المركزية لجامعة قسنطينة2	8
22	المكتبة المركزية لجامعة قسنطينة3	10
المجموع	22 مكتبة مركزية	429

1.2.2.1عينة الدراسة:

تم الإعتماد في الدراسة على العينة الغير عشوائية القصدية، شملت جميع موظفي المكتبات المركزية التابعة لجامعات الشرق الجزائري تخصص؛ علم المكتبات على إختلاف درجاتهم العلمية ورتبهم الإدارية. والجدول الموالي يوضح توزيع الردود المستلمةحسب كل مكتبة مركزية من المكتبات الجامعية محل الدراسة. الجدول رقم (02) يوضح عدد الفعلي للعينة الأساسية للدراسة:

الجدول رقم(02): يمثل عينة الدراسة

الرقم	الجامعة	التكرار	النسبة المئوية%
01	المكتبة المركزية لجامعة الشهيد العربي التبسي–تبسة	4	%3,6
02	المكتبة المركزية لجامعة باتنة1–الحاج لخضر	11	%10
03	المكتبة المركزية لجامعة فرحات عباس –سطيف1	13	%11.8
04	المكتبة المركزية لجامعة الهضاب –سطيف2	10	%9,1
05	المكتبة المركزية لجامعة الأمير عبد القادر –قسنطينة1	6	%5,5
06	المكتبة المركزية لجامعة محمد ميرة –جيجل	7	%6,4
07	المكتبة المركزية لجامعة الاخوة منتوري –قسنطينة1	12	%10,9
08	المكتبة المركزية لجامعة الشاذلي بن جديد –الطارف	3	%2,7
09	المكتبة المركزية لجامعة ام البواقي	11	%10
10	المكتبة المركزية لجامعة سوق هراس	2	%1,8
11	المكتبة المركزية لجامعة عنابة	5	%4,5

12	المكتبة المركزية لجامعة 8 ماي1945 –قالمة	5	%4,5
13	االمكتبة المركزية لجامعة المسيلة	7	%6,4
14	المكتبة المركزية لجامعة ورقلة	6	%5,5
15	المكتبة المركزية لجامعة برج بوعريريج	5	%4,5
16	المكتبة المركزية لجامعة قسنطينة3	3	%2,7
17	المكتبة المركزية لجامعة سكيكدة	00	/
18	المكتبة المركزية لجامعة قسنطينة 2	00	/
	المجموع	110	%100

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يمثل **الجدول رقم(02)**، العينة الفعلية للدراسة؛ وقد بلغ العدد الإجمالي 110مكتبي مختص في علم المكتبات والمعلومات من إجمالي 148 مفردة بحث، موزعين على 18 مكتبة مركزية؛ حيث أن (N=148).

وتجدر الإشارة إلى أن عدد الردود المتحصل عليها بعد توزيع الإستبيان النهائي علىالعينة هو**118 رد**، سجلنا فقدان **08 ردود** رغم محاولات الإرسال المتكررة عن طريق أكثر من وسيلة إتصال؛ في حين لم يتم تسجيل أي ردود لكل من المكتبة المركزية لجامعة سكيكدة والمكتبة المركزية لجامعة قسنطينة 2، كما تم إستثناء المكتبات المركزية الأربع (**04**) المتعلقة بالدراسة الإستطلاعية ممثلة في: المكتبة المركزية جامعة بسكرة، المكتبة المركزية جامعة باتنة 2، والمكتبة المركزية جامعة الوادي، والمكتبة المركزية جامعة خنشلة.وعليه بلغ عدد مفردات العينة المشاركة بشكل فعلي في هذه الدراسة هو (N=110).

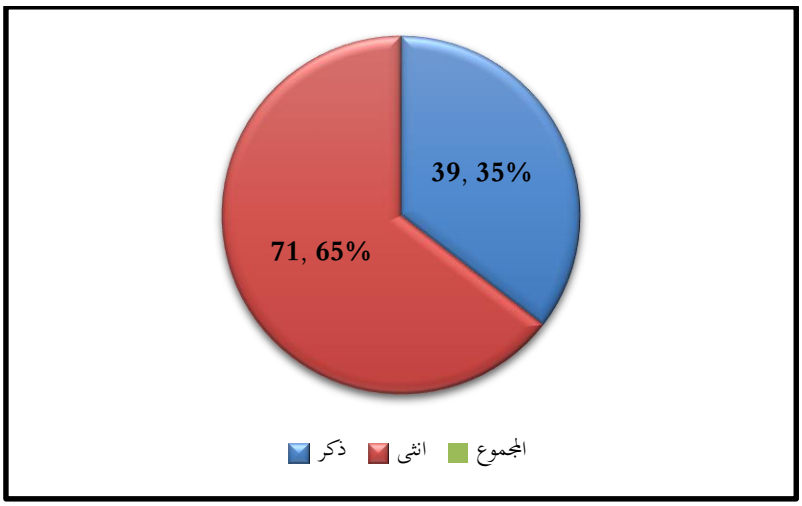
ويجدر الإشارة أن إختيار الباحث لعينة الدراسة نتيجة شروط محددة وهي كالآتي:

- توسيع مجال الدراسة لجامعات الشرق الجزائري يظهر تنوع سياسات الجامعة في مجال الحوكمة.
- موقع المكتبات المركزية في التنظيم الإداري في الجامعات الجزائرية.
- تحديد الفروقات السوسيوديموغرافية للأخصائي المعلومات بالمكتبات المركزية؛ جامعات الشرق الجزائري.

1.1.2.2.1خصائص عينة الدراسة:

خصائص عينة الدراسة تتحدد في البيانات الشخصية لمفردات البحث، وشملت الخصائص عدة مؤشرات (الجنس؛ مكان العمل؛ المستوى العلمي؛ الرتبة؛ الخبرة)؛ نورد نتائجها في العناصر التالية:

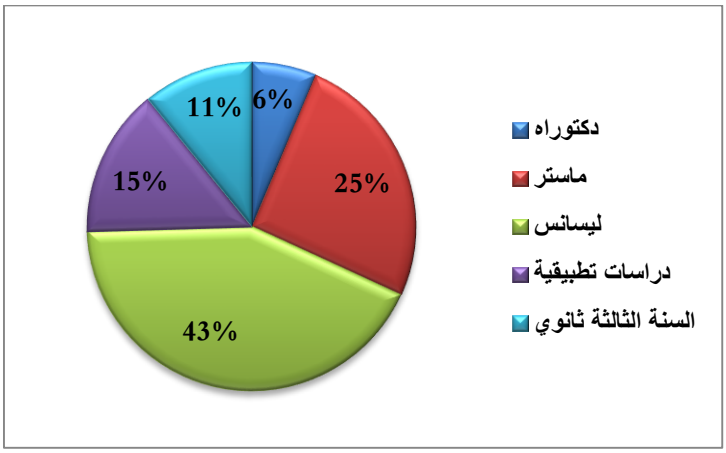
أ. توزيع عينة الدراسة حسب الجنس:



الشكل رقم (01) توزيع عينة الدراسة حسب الجنس

نلاحظ من خلال الشكل رقم(01) أن ما نسبته 64.5% من عينة الدراسة إناث، بينما 39% ذكور. ويرجع الباحث الزيادة في نسبة الإناث إلى واقع التوظيف في مكتبات الشرق الجزائري؛ حيث تشكل النساء غالبية العاملين خاصة في الخدمات المرتبطة بالمستفيدين والمعالجة الفنية.

ب.توزيع العينة حسب المستوى العلمي:



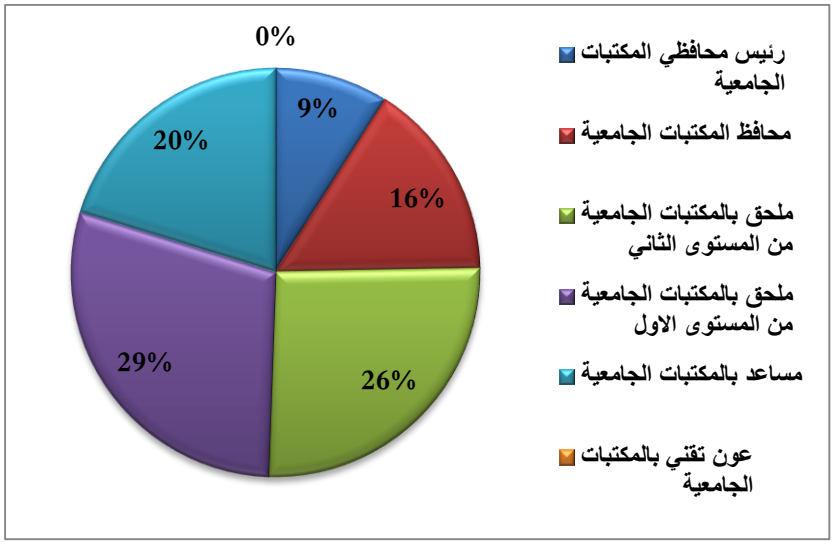
الشكل رقم (02): توزيع عينة الدراسة حسب المستوى العلمي

يتضح من الشكل رقم (02): أن الأفراد الحاصلين على شهادة الليسانس يشكلون النسبة الأعلى من عينة الدراسة بنسبة 42.7% (47 فردًا) ، يليه الأفراد الحاصلين على شهادة الماستر بنسبة 25.5 (28فرد)، أما الأفراد الحاصلين على درجة الدكتوراه يشكلون أقل نسبة بنسبة 6.4% .

يعكس هذا التوزيع هيمنة الفئة ذات المستوى الجامعي المتوسط داخل مكتبات الشرق الجزائري، وهو ما يتوافق مع طبيعة مناصب العمل التي لا تشترط غالبًا مستويات أكاديمية عليا، بل تركز على المهارات التطبيقية والخبرة المهنية.

يُعد المستوى العلمي من المتغيرات المهمة التي قد تُفسر تفاوت درجة الوعي والتمكن في التعامل مع التحديات المرتبطة بالأمن السيبراني، ومستوى الفهم لإجراءات الحوكمة، وإستخدام البرمجيات المؤمنة، وتقييم فعالية نظم حماية المعلومات.إذ من المتوقع أن يكون لحاملي الشهادات العليا (ماستر ودكتوراه) وعي نظري ومهاري أعلى بمخاطر الاختراقات ووسائل الحماية الرقمية، مقارنة بمن هم في مستويات تعليمية أقلوالذي هم بحاجة الى تعزيز كفاءتهم في التعامل مع الأنظمة الرقمية المعتمدة في المكتبات الجامعية.

ج.توزيع العينة حسب الرتبة الإدارية:

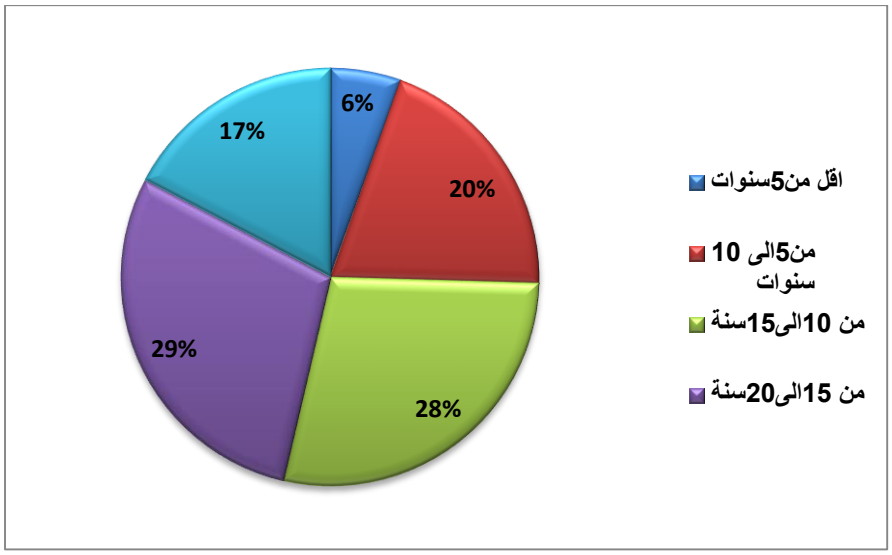


الشكل رقم (03): توزيع العينة حسب الرتبة الإدارية

يوضح الشكل رقم (03) أن عينة الدراسة تتسم بتنوع الرتب الوظيفية داخل المكتبات الجامعية، حيث نجد أنرتبة ملحق المكتبات الجامعية من المستوى الثاني النسبة الأكبر بـ23.6%، تليهم فئة رتبة ملحق بالمكتبات الجامعية المستوى الأول بنسبة 20.9%، ثم مساعد بالمكتبات الجامعية بنسبة 19.1.%، في حين بلغت نسبة الأعوان التقنيين 16.4%. أما الرتب العليا فقد كانت أقل تمثيلًا، حيث بلغت نسبة محافظي المكتبات الجامعية 12.7%، ورؤساء المحافظين 7.3.%

يعكس هذا التوزيع الواقع الهيكلي للمكتبات الجامعية، والذي يتميز بسيطرة الرتب الوسطى والدنيا عددًا على الجهاز الوظيفي، مقابل محدودية الرتب العليا في الهرم الإداري. هذا التركيب له دلالات مهمة في أمن المعلومات والحوكمة، إذ من المتوقع أن تختلف درجة الوعي بالمخاطر السيبرانية ومستوى الالتزام بالإجراءات التنظيمية باختلاف المسؤوليات والمهام المرتبطة بكل رتبة. فمثلًا، قد تكون الفئات الإدارية العليا (كرؤساء المحافظين والمحافظين) أكثر اطلاعًا على السياسات الأمنية والاستراتيجيات العامة، في حين تنحصر مهام الأعوان والفئات التقنية في تنفيذ التعليمات دون بالضرورة إدراك خلفياتها أو أبعادها الأمنية.

د.توزيع العينة حسب سنوات الخبرة:



الشكل رقم (04): توزيع العينة حسب سنوات الخبرة

تشير معطيات الشكل رقم (04) إلى أن أكبر نسبة من أفراد العينة تقع ضمن فئتي "من 15 إلى 20 سنة" بنسبة 29.1% و"من 10 إلى 15 سنة" بنسبة 28.2%، مما يعني أن أكثر من نصف العينة (57.3%) تتمتع بخبرة مهنية تتجاوز عشر سنوات. بينما توزعت النسب المتبقية بين فئة "من 5 إلى 10 سنوات" بـ20%، وفئة "أكثر من 20 سنة" بـ17.3%، وأخيرًا فئة "أقل من 5 سنوات" بنسبة 5.5% فقط.

يعكس هذا التوزيع أن عينة الدراسة يغلب عليها أصحاب الخبرة المهنية، حيث يشكل الموظفون ذوي الخبرة المتوسطة إلى الطويلة النسبة الأكبر، وهو مؤشر مهم في سياق تحليل مدى إدراك العاملين بالمكتبات الجامعية لقضايا الحوكمة والمخاطر السيبرانية. فمن الناحية النظرية، يُفترض أن الخبرة المهنية تسهم في تراكم المعرفة بالممارسات التنظيمية والتقنية، وكذلك تطوير الحس الأمني في التعامل مع نظم المعلومات. ومع ذلك، قد يُظهر التحليل أن الموظفين الأقدم لا يمتلكون بالضرورة وعيًا أعلى بالمخاطر السيبرانية، خاصة إذا لم يصاحب خبرتهم تكوين دوري أو تحديث لمعارفهم في ظل تطور التهديدات الرقمية.

3.2.1 أدوات جمع البيانات

تعد أدوات البحث العلمي من أساسيات البحث التي يجب على الباحث الإلمام بها ومعرفتها، تشير أدوات البحثالوسائل والطرق والأساليب المختلفة التي يعتمد عليها في الحصول على المعلومات والبيانات اللازمة لإنجاز البحث. ولجمع البيانات اللازمة للإجابة على تساؤلات وفرضيات الدراسة. تم الإعتماد في الدراسة على أداتين أساسيتين وهي:

1.3.2.1 أداة الملاحظة

أعتمد الباحث على أداة الملاحظةأثناء الزيارات الميدانية للمكتبات المركزية محل الدراسة، وتمثلت فائدة هذه الأداة في البحث في الإستعانة بما تم ملاحظته في تحليل وتفسير البيانات المتعلقة بإجابات أفراد العينة في أداة البحث

2.3.2.1 أداة الإستبيان

إعتمد الباحث على أداة الإستبيان في جمع البيانات ذات الصلة بالموضوع، شملت الدراسة مجموعة من العبارات يتم الإجابة عنها وفق مقياس ليكرت الخماسي، تم توزيعها على أفراد عينة الدراسة عن طريق الزيارة الفعلية لعدد من المكتبات محل الدراسة وأيضا البريد الإلكترونية .

تم إعداد الإستمارة بناء على أهداف الدراسة، وتقديمها لمجموعة من المحكمين من داخل الوطن.

بعد إطلاع المشرف وباقي المحكمين على الاستمارة تم إعطاء الملاحظات والتصويبات، خضعت الدراسة إلى الإختبار على عينة من المبحوثين ممثل في الدراسة الإستطلاعية،تتكون العينة من المكتبيينبالمكتبة المركزية لجامعة خنشلة، والمكتبة المركزية جامعة بسكرة، والمكتبة المركزية جامعة باتنة2، والمكتبة المركزية جامعة الوادي.

في الأخير، تم إخراج الاستبيان في شكله النهائي وتوزيعه عل العينة الفعلية للدراسة.

تم تقسيم الإستبيان الى أربع محاور رئيسية يحتوي كل محور منها على مجموعة من الأسئلة على النحو الموالي:

محور البيانات الشخصية.

المحور الأول: وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني.

المحور الثاني: حوكمة المعلومات

المحور الثالث: مخاطر الأمن السيبراني

المحور الرابع: أثر حوكمة المعلومات على مخاطر الأمن السيبيراني.

1.2.3.2.1 إختبار أداة الإستبيان

أولا: إختبار التوزيع الطبيعي

تم إختبار التوزيع الطبيعي بإستخدام إختبار كولمجروف – سمرنوف(1-sample K-S)

تم إجراء إختبار كولموغوروف–سميرنوف لعينة واحدة (One-Sample Kolmogorov–Smirnov Test) للتحقق من مدى إتباع بيانات محاور الدراسة للتوزيع الطبيعي، وهو إختبار ضروري لأن معظم الإختبارات المعلمية تشترط أن يكون توزيع البيانات طبيعي، كما يوضحه الجدول أدناه:

الجدول رقم (03) : إختبار التوزيع الطبيعي (1- samplekolmogorov – smirnov)

المحور	عنوان المحور	عدد الفقرات	قيمة z	القيمة الاحتمالية
الأول	وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني.	10	0.098	0.200*
الثاني	حوكمة المعلومات	24	0.085	0.200*
الثالث	مخاطر الأمن السيبراني	28	0.092	0.200*
الرابع	أثر حوكمة المعلومات على مخاطر الأمن السيبراني	12	0.113	0.200*

المصدر: من إعداد الباحث بإستخدام برنامج SPSS

أظهرت النتائج أن القيم الإحتمالية لجميع المحاور جاءت أكبر من مستوى الدلالة المعتمد (0.05)، حيث بلغت Sig = 0.200لكل محور (مع تصحيح ليلييفورز)، مما يدل على عدم وجود فروق دالة بين توزيع البيانات والتوزيع الطبيعي. وعليه يمكن إعتبار بيانات محاور الدراسة متبعة للتوزيع الطبيعي، وبالتالي تم اعتماد الاختبارات المعلمية في تحليل البيانات وإختبار الفرضيات.

ثانيا: تحليل فقرات الدراسة

تم إستخدام إختبار T للعينة الواحدة (one sample Ttest)لتحليل فقرات الإستبيان، تكون الفقرة إجابية بمعنى أن أفراد العينة يوافقون على محتواها إذا كانت قيمة Tالمحوسبة أكبر من قيمة T الجدولية والتي تساوي 1.98 (أو القيمة الإحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أكبر من60%)، وتكون الفقرة السلبية بمعنى أن أفراد العينة لا يوافقون على محتواها إذا كانت قيمة T المحوسبة أصغر من قيمة T الجدولية والتي تساوي -1.98 (أو القيمة الإحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أقل من60%)، وتكون آراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من0,05 .

خلاصة الفصل:

تم تحديد الأبعاد المنهجية للدراسة وركائز الدراسة الميدانية، وسيتم التفصيل فيه في الجانب التطبيقي؛ الفصل الخامس والفصل السادس. إضافة إل ذلك تم تقسيم الجانب النظري للدراسة إل فصول فرعية مترابطة ومتكاملة مع بعضها البعض لمعالجة حوكمة المعلومات ومخاطر الأمن السيبراني في المكتبات الجامعية في جوانب عدة.

الفصل الثاني:

المقاربات النظرية لحوكمة المعلومات

تمهيد:

تمثل حوكمة المعلومات أحد أبرز التوجهات الحديثة في وقتنا الراهن من الناحية الأكاديمية والعملية. ولقد نتاولت العديدة من الدراسات والأبحاث موضوع حوكمة المعلومات وأطر تنفيذها في المؤسسات، وفي هذا الفصل سيناقش الجذور النظرية والمفاهيمية لمصطلح حوكمة المعلومات، المفاهيم ذات الصلة، كما تسلط الضوء عل دوافع التوجه لتطبيق حوكمة المعلومات وأدوارها في المؤسسة والأهداف المتوقعة بعد تنفيذها، كما يناقش الفصل مبادئ وأبعاد حوكمة المعلومات.

1.2 حوكمة المعلومات: الجذور النظرية والتأصيل المفاهيمي

1.1.2 مفهوم حوكمة المعلومات

1.1.1.2 تعريف الحوكمة:

أ. لغة:

يأتي مصطلح الحوكمة من المنظور اللغوي من "الفعل حكم الذي يعني سيطرة، أدار، وهيمن أو احتوى، أو مارس السلطة"[1]، وهو مستحدثا من قاموس اللغة العربية وهو ما يطلق عليه النحت في اللغة. واللفظ مستمد من الحوكمة وهو ما يعني الانضباط والسيطرة والحكم بكل ما تعني هذه الكلمة من معاني، وعليه فأن لفظ الحوكمة يتضمن العديد من الجوانب منها:

1. الحكمة: ما يقتضيه من التوجيه والإرشاد.
2. الحكم: وما يقتضيه من السيطرة على الأمور بوضع الضوابط والقيود التي تتحكم في السلوك.
3. الإحتكام: وما يقتضيه من الرجوع الى المرجعيات أخلاقية وثقافية وإلى خبرات تم الوصول عليها من خلال تجارب سابقة.
4. التحاكم: طلبا للعدالة خاصة عند إنحراف سلطة الإدارة وتلاعبها بمصالح المساهمين[2].

---

[1]. شنافي، كفية. **آليات ومبادئ الحوكمة في شركات التأمين: دراسة مقارنة بين الشركة الجزائرية للتأمين CAAR وشركة AXA**. مجلة كلية بغداد للعلوم الاقتصادية. العدد، 45، 2015. ص 337

[2]. يعقوب عادل، ناصر الدين. **إطار نظري مقترح لحوكمة الجامعات ومؤشرات تطبيقها في ضوء متطلبات الجودة الشاملة.** مجلة تطوير الأداء الجامعي. المجلد، 01. العدد، 02، 2012. ص 89

من التعريف اللغوي نستنتج أن الحوكمة قائمة على المنطق والنقد والعقلانية في تسيير وإدارة شؤون الفرد والمؤسسة مبنية على مرجعية وظوابط محددة.

يعود ظهور ونشأة هذا المصطلح تاريخيا لفترة طويلة فمصطلح الحوكمة ذو أصل يونانيKbueman وعرف باللاتينية Gubernare وكان يستخدم في الفرنسية القديمة في القرن الثالث عشر كمرادف لمصطلح الحكومة Governomment، وانتقل الى اللغة الإنجليزية في القرن الرابع عشر Governance.[1]

ب. اصطلاحا:

ورد في الأدبيات الإقتصادية والسياسية والإجتماعية العديد من التعريفات المتعلقة بمصطلح الحوكمة؛متخصصين خبراء وكذلك المؤسسات والمنظمات الدولية. ومن أهم هذه التعريفات نذكر ما يلي:

تعرف منظمة التعاون الاقتصادي والتنمية OECDالحوكمة بأنها: "مجموعة من العلاقات التي تربط بين القائمين على إدارة الشركة ومجلس الإدارة وحملة الأسهم وغيرهم من أصحاب المصالح".[2]

كما تعرف بأنها: "مجموعة القوانين والنظم والقرارات التي تهدف إلى تحقيق التميز في الأداء عن طريق تحقيق أساليب مناسبة وفعالة لتحقيق خطط وضبط الأهداف".[3]

ومن خلال ما ورد في المفاهيم السابقة نستنتج أن الحزوكمة تتجسد في إدارة شؤون المؤسسة في البيئة الداخلية وخارجها بمجموعة قوانين وعلاقات وظوابط تعزز قرارات المؤسسة من جهة وتحقق مبدأ التواصل الفعال بين جميع الأطراف.

حيث يعرف Hewitt وCynthiaالحوكمة بأنها:"القدرة على تسيير الفعال لكل المنظمات ويتجلى ذلك في أخذ القرارات الملائمة بدقة والبحث عن الديناميكية على مستوى النشاط الجماعي لخدمة الصالح العام والخاص".[4]

---

[1] .سرير عبد الله،ناذير ؛ رحمونة، بوشتة. **حوكمة المعلومات والوثائق في المؤسسات وأزمة كورونا**. مجلة الاقتصاد والتنمية البشرية. المجلد.12، العدد،02، 2021. ص 16

[2].Makhlouf Shabou, Basma. **Information Governance**, **European Public Administrations**. Ala- Ica conference. Mexico City,28 November, 2017.P04

[3]. بن خضير، أحمد بن عبد الله. **حوكمة المعلومات مبادئ، استراتيجيات وأفضل الممارسات**. دار جامعة الملك سعود للنشر. الرياض،1442. ص 07

[4]. غالم جلطي، العربي بوزيان. **مفهوم الحوكمة: عوامل ظهورها ومرتكزاتها، ومجالات استخداماتها**. مجلة المالية والأسواق. المجلد،08. العدد،92، 2021. ص440

ويعرفها البرنامج الإنمائي للأمم المتحدة: UNDP:" الحوكمة هي ممارسة السلطة الاقتصادية والسياسية والإدارية، لإدارة شؤون الدولة على كافة المستويات ويشمل الآليات والعمليات والمؤسسات التي من خلالها يعبر المواطنون والمجموعات عن مصالحهم ويمارسون حقوقهم القانونية ويوفون بالتزاماتهم ويقبلون الوساطة لحل خلافاتهم.[1]

مما سبق ذكره يمكن تعريف الحوكمة إجرائيا بأنها: الممارسة الرشيدة لسلطات الإدارة، وعملية صنع القرار من خلال الارتكاز على القوانين والمعايير والقواعد المنضبطة التي تحدد العلاقة بين المؤسسة والأطراف المرتبطة بالمؤسسة والتي تشجع على الإستخدام الأمثل للموارد وتوفير نظم المحاسبة والمساءلة.

2.1.1.2 تعريف المعلومات:

أ.لغة:

المعلومات لغة: مشتقة من الفعل علم، وتدل على الإحاطة بمواطن الأمور والوعي، والادراك. وتعني الإستيعاب والخبرة والاتقان بالتعلم أي القدرة على التمييز والتعليم والتعلم والدراسة[2].

ب.إصطلاحا:

وردت تعريفات عدة لمصطلح المعلومات نذكر منها:

المعلومات هي "عبارة عن بيانات تكون على شكل ألفاظ أو رموز أو أرقام، كالبيانات التي تمت معالجتها وتحولت إلى معلومات مفهومة تساعد في إتخاذ القرارات بشكل يقلل من حدوث المخاطر عند متخذي القرار وذلك من خلال مجالات أداة الدراسة؛ الدقة، المرونة ،الشمول، الملائمة، والتوقيت المناسب للمعلومات". [3]

كما تعرف بأنها: تلك البيانات التي تم معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي البيانات التي أصبحت لها قيمة بعد تجميعها وتنظيمها في شكل معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية أو في أي شكل. [4]

---

[1]. الشامي، حسين علي. **الحوكمة والنمو الاقتصادي دراسة في دول مختارة مع إشارة خاصة للعراق**. دار غيداء. عمان. ط،01، 2019. ص 28

[2]. الصباغ،عماد عبد الوهاب. **علم المعلومات**. دار الثقافة والنشر والتوزيع. الأردن، 2004.ص30

[3]. عظيمي، أحمد؛ زغنوف،عبد الغني. **المعلومة وأهميتها في المجتمع المعلوماتي**. مجلة البحوث والدراسات الإنسانية. المجلد،08. العدد،09، 2014. ص194

[4]. عبد الهادي،محمد فتحي. **المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديد**. مكتبة الدار العربية للكتاب. مصر، 2000.ص 19

وتعرف المعلومة في المؤسسة على أنها " التجميع والتشكيل والنشر على شكل معلومات تقنية، اقتصادية، إجتماعية، ضرورية كانت أو غير ضرورية مع إعلام الموظفين بها كي يتسنى لكل فرد من أفراد المؤسسة الإطلاع عليها لتكون ذات فائدة وتساهم بفاعلية في إتخاذ القرار السليم. [1]

وفي ضوء ما سبق ذكره نخلص أن المعلومات عبارة عن تجميع وتحليل البيانات ممثلة في المدخلات الأولية يتم معالجتها وغربلتها وتحليلها للحصول على معلومات، هذه الأخيرة تستخدم بدورها كمدخلات رئيسية في عملية اتخاذ القرار. والمعلومة لابد أن تتوفر على جملة من الخصائص حتى تكون ذات فائدة وتساهم في إتخاذ القرار السليم.

3.1.1.2 تعريف حوكمة المعلومات:

حوكمة المعلومات **IG**هي أحد فروع حوكمة الشركات وتتضمن مفاهيم أساسية من إدارة السجلات وإدارة المحتوى وتقنية المعلومات وحوكمة البيانات وأمن المعلومات وخصوصية البيانات وإدارة المخاطر والجاهزية للرد على الدعاوى القضائية والإمتثال للقوانين واللوائح وحفظ السجلات الرقمية وحتى ذكاء الأعمال.[2]

كما تعرف شركة *Gartner Inc مصطلح حوكمة المعلومات بأنها: "تحديد الحقوق المنوطة بالقرار وإطار المساءلة لضمان السلوك المناسب في إنشاء المعلومات، تخزينها وتقييمها وأرشفتها وحذفها. وهو يتضمن العمليات والأدوار والسياسات والمعايير والمقاييس التي تضمن الإستخدام الفاعل والكفء للمعلومات، بما يمكن المؤسسة من تحقيق أهدافها".[3]

تعرف الجمعية الدولية لمديري ومسؤولي إدارة السجلات ARMA حوكمة المعلومات أنها:"إطار عمل إستراتيجي مكون من المعايير والعمليات والأدوار والمقاييس التي تجعل المؤسسات والأفراد مسؤولين عن توليد المعلومات وتنظيمها وتأمينها وحفظها وإستخدامها والتخلص منها بطرق تتناسب مع أهداف المؤسسة وتساهم في تحقيقها". [4]

***شركةGartner Inc**: أحد أبرز الشركات العالمية المتخصصة في أبحاث وإستشارات تكنولوجيا المعلومات، تأسست عام 1979 من طرف جيفري غارتنر بستامفورد؛ الولايات المتحدة الأمريكية، تعد مرجعا رئيسيا للمؤسسات في حوكمة المعلومات وإدارة البيانات وظيفتها: تقديم أطر وإستراتجيات حوكمة المعلومات وأدوات إدارة البياناتبالمؤسسة.

1. A. R François. **Manuel de l'organisation de l'entreprise**. Les Edition de l'organisation. N (07), 1988. P 101

2. Makhlouf Shabou, Basma.**OP**.**Cit**, P04

3. سرير عبد الله،ناذير؛ رحمونة، بوشتة.**المرجع السابق**. ص 26

4 . بن خضير، أحمد بن عبد الله.**المرجع السابق**.ص 08

أيضا حوكمة المعلومات هي: فن التفاعل الموجود بين أصحاب المصلحة الرئيسيين في برنامج IG (تكنولوجيا المعلومات والأعمال والشؤون القانونية والإمتثال والأمن والخصوصية) بهدف التقليل من مخاطر المعلومات على المؤسسة مع تعظيم قيمة أصول المعلومات من خلال بناء السلوكيات المرغوبة وتمكين إتخاذ قرارات متعددة الوظائف.[1]عرفها أيضا F. Robert أنها:"نوع من الإنضباط الفائق الذي ظهر نتيجة للتشريعات الجديدة والمشددة التي تحكم الأعمال والتهديدات الخارجية مثل القرصنة وإنتهاكات البيانات، والإعتراف بأن هناك حاجةإلى تخصصات متداخلة ومتعددة لمعالجة تحديات إدارة المعلومات اليوم في بيئة أعمال منظمة بشكل متزايد ومقاضاته".[2]

أما المعهد الأسترالي للحوكمة* فقد عرفها بأنها "النظام الذي يتم من خلال توجيه ورقابة الإستخدامات الحالية والمستقبلية لتقنية المعلومات، وتقييم وتوجيه الخطط لإستخدام تقنية المعلومات في تدعيم المنظمة ومتابعة هذا الإستخدام لإنجاز الخطط والأهداف المقررة".[3]

تعريفإجرائي لحوكمة المعلومات يمكننا القول إنها عبارة عن تنسيق لممارسات إدارة المعلومات خلال دورة حياتها، بمعنى أنها تضبط الإطار التنظيمي والإستراتيجي لتحديد الأدوار والأعمال من أجل التحكم في الوثائق المطبوعة والرقمية بهدف التقليل من المخاطر والتكاليف المرتبطة بها.

• **المعهد الأسترالي للحوكمة** هي جمعية عضوية وطنية متخصصة في الحوكمة وإدارة المخاطر بأستراليا تأسست عام 1909، تزود أكثر من 7500 عضو بالأدوات اللازمة لتحسين الحوكمة داخل مؤسساتهم، كما تعنى بإعداد برامج حوكمة المعلومات، إعداد الأدلة والمنشورات وتنظيم دورات تكوينية ودعم المشاريع البحثية في المجال.

[1]. Done White. John MC Manus. Andrew Atherton. **Governance and information, Governance some Ethical considerations within an expanding information Society**. University of Lincoln. Faculty of business and law: Brayford Pool. England, 2004.P 05

[2]. بن خضير، أحمد بن عبد الله. **المرجع السابق**. ص 06

[3].حازم يحي، منى. **أثر حوكمة المعلومات في تعزيز المستوى التعليمي لطلبة الدراسات الأولية والدراسات التطبيقية**. مجلة الآداب. المجلد،132.، 2020.ص 176

2.1.2 حوكمة المعلومات والمفاهيم المرتبطة به:

1.2.1.2 حوكمة تكنولوجيا المعلومات:

تؤكد أدبيات موضوع حوكمة المعلومات على أن المصطلح ظهر لأول مرة في أوائل التسعينيات من القرن الماضي، للدلالة على الآليات التي تضمن تحقيق القدرات اللازمة لتكنولوجيا المعلومات، لكن لم يتم معالجته مباشرة إلا في وقت لاحق من هذا العقد.وتظهر بعض الدراسات التي تشير إلى مصطلح حوكمة تكنولوجيا المعلومات ITGعلى سبيل المثال دراسةBrown and Grant 2005، إضافة الى تأسيس معهد حوكمة تكنولوجيا المعلومات سنة 1998؛ وهو منظمة صناعية تهدف إلى بناء وتعزيز فكرة وممارسات حوكمة تكنولوجيا المعلومات حول العالم، وتعزز الاهتمام بها أكثر مع التوجه العالمي نحو حوكمة المعلومات المؤسسات نتيجة للأزمات والفضائح المالية التي ضربت شركات ومؤسسات عالمية مثل: شركتي Enron وWorldComالأمريكية سنة 2002.[1]

في مجال العلوم الإنسانية والاجتماعية أستخدم مصطلح حوكمة تكنولوجيا المعلومات حديثا، على الرغم من أن المفهوم قد إستعمله بعض الباحثين في تطبيق آليات ضبط وتقييم تكنولوجيا المعلومات في المنظمات منذ فترة طويلة وبمفاهيم مختلفة، كآليات إدارة منظومة الكمبيوتر ومسؤولية إتخاذ القرارات المتعلقة بتكنولوجيا المعلومات والتحكم فيها. فنجد معهد حوكمة تكنولوجيا المعلومات يرى أنها مسؤولية مجلس الإدارة والإدارة التنفيذية، كما أنها جزء لا يتجزأ من حوكمة المؤسسةتتكون من الهياكل والعمليات القيادية والتنظيمية التي تضمن أن تكنولوجيا المعلومات بالمنظمة تدعم وتوسع إستراتيجيتها وأهدافها.[2]

وفي السياق نفسه يعرفها معيار حوكمة المنظمات لتكنولوجيا المعلومات ISO/IEC 38500 بأنها نظام الذي يتم من خلاله توجيه الإستخدام الحالي والمستقبلي لتكنولوجيا المعلومات والتحكم فيه، حيث يشمل تقييم وتوجيه إستخدام تكنولوجيا المعلومات لدعم المنظمة ومراقبة هذا الإستخدام لتحقيق الهدف منه، كما يشمل سياسات وإستراتيجيات المعلومات داخل المنظمة.[3]

---

[1]. بركات، عبد الرزاق؛ بن حاوية، أمينة. **حوكمة تكنولوجيا المعلومات واليات تنفيذها وتقييمها في المكتبات**. مجلة العلوم الاجتماعية والإنسانية. المجلد،22. العدد،02، 2021.ص 687

[2]. بركات، عبد الرزاق؛ بن حاوية، أمينة. **المرجع نفسه**. ص 688

[3]. Zahi, Jamal ;Belhaj,Aadil. **La gouvernance des technologies de l'information : un dispositif de contrôle du système d'information éducation**. Revue repères et perspectives économiques. V (02). N (02), P 97

إجتمعت العديد من العوامل التي أظهرت أهمية التفكير الجدي في التوجه نحو تنفيذ حوكمة تكنولوجيا المعلومات، بعد تزايد التركيز على فهم أساسيته ومتطلباته ومزاياه من طرف الهيئات ومديري المنظمات والتي تتمثل في:

_ التوجه العالمي نحو الحوكمة جراء الأزمات الاقتصادية والمالية.

_ التطور الكبير والسريع لتكنولوجيا المعلومات والتكاليف الباهظة التي تتطلبها.

_ الدور الحاسم لتكنولوجيا المعلومات داخل المنظمة وتحولها من مجرد أداة لأتمتة الإجراءات إلى أداء فعالة لصنع القرارات الاستراتيجية.

_ فشل أغلب المؤسسات على الحصول على عوائد مرضية من توظيفها لتطبيقات تكنولوجيا المعلومات نتيجة ضعف التخطيط.

_ التهديدات والمخاطر المرتبطة بتكنولوجيا المعلومات التي قد تؤثر على أمن المعلومات المؤسسة، وبالتالي تأثيرها على سمعتها وتنافسيتها[1].

ومن هنا يمكن القول تهدف حوكمة تكنولوجيا المعلومات إلى تحقيق هدفين رئيسيين كالآتي: إستخدام تكنولوجيا المعلومات بشكل إستراتيجي لتحقيق أهداف المنشأة والمنافسة الفعالة، وإدارة مصادر تكنولوجيا المعلومات في الشركة بكفاءة وفعالية والرقابة على أمن تكنولوجيا المعلومات.

2.2.1.2 حوكمة المؤسسات:

تعد حوكمة المؤسسات من أهم الموضوعات في المؤسسات والمنظمات الإقليمية والدولية حيث إزداد الاهتمام في الآونة الأخيرة بمفهوم حوكمة المؤسسات، وهذا راجع الى إتساع حجم المشروعات مما أدى إلى إنفصال الملكية عن الإدارة، وأيضا ضعف آليات الرقابة على تصرفات المدراء مما أدى إلى حصول أزمات إقتصادية نذكر على سبيل المثال: أزمة جنوب شرق أسيا في أواخر التسعينات.[2]

---

[1] . بركات، عبد الرزاق؛ حاوية، أمينة. **حوكمة تكنولوجيا المعلومات: وسيلة للتحكم في مشاريع تكنولوجيا المعلومات في المكتبات الجامعية**. مجلة الناصرية للدراسات الاجتماعية والتاريخية. المجلد،12. العدد،02، 2021.ص 570

[2]. بن عمر، محمد البشير؛ دادن، عبد الغني. **حوكمة المؤسسات ودورها في تحسين أداء المؤسسة**. مجلة الدراسات الاقتصادية والمالية. المجلد،01. العدد،07، 2014. ص 25

كما أن ظهور حوكمة المؤسسات يرجع إلى عوامل عدة وهي:

- ظهور مفهوم الخصخصة إستدعى وضع معايير تحمي سلامة أوضاع المؤسسات التي تمت خصخصتها.
- إهتمام حقوق أصحاب المصالح في سلوكيات ممارسة الإدارة في الشركات.
- عدم تحديد مسؤولية مجلس الإدارة ومهام إدارة الشركة تجاه أصحاب المصالح والمساهمين.
- تحرير الأسواق المالية، وتزايد إنتقال رؤوس الأموال عبر الحدود بشكل كبير وبحث الشركات عن مصادر للتمويل بأقل تكلفة.
- تأثير بعض الدراسات التي قدمت في مجال حوكمة الشركات في بريطانيا وأمريكا.
- مشكلة إنفصال الملكية عن الإدارة وظهور نظرية الوكالة، وحماية حقوق صغار المساهمين والأطراف الأخرى ذات الصلة بالشركة[1].

كما تعرف:"حوكمة المؤسسات بأنها القواعد والمعايير التي تحدد العلاقة بين إدارة المؤسسة وحملة الأسهم والسندات وأصحاب المصالح والأطراف المرتبطة بالمؤسسة وذلك النظام الذي يتم من خلاله إدارة وتوجيه وتنظيم مراقبة المؤسسات والإجراءات التي توجه وتدير المؤسسات وتراقب أداؤها بحيث تضمن الوصول إلى تحقيق الرسالة والأهداف المرسومة لها "[2]، وبذلك تضمن مصالح جميع الأطراف: المدراء، والمستخدمون، والزبائن، والمراقبون، وأصحاب المصالح، والمساهمون والمجتمع.

ولحوكمة المؤسسات أهمية بالغة لما لها تأثير مباشر في جذب الاستثمارات سواء كانت وطنية أو أجنبية وفقا لضوابط مقررة سابقا تفاديا للفساد الذي قد يشوب عمليات التسيير من قبل المسيرين.وترجع أهمية حوكمة المؤسسات إلى العمل على كفاءة إستخدام الموارد وتعظيم قيمة المؤسسة وتدعيم تنافسيتها في الأسواق بما يمكنها من جذب مصادر التمويل محلية وعالمية للتوسع والنمو، وأيضا يجعلها قادرة على خلق فرص جديدة، مع الحرص على تدعيم استقرار أسواق مالية والأجهزة المصرفية، مما يؤدي الى تحقيق الكفاءة والتنمية الاقتصادية المطلوبة.[3]

---

[1]. بن عمر، محمد البشير؛ دادن، عبد الغني. **المرجع السابق**. ص 27

[2] . سليمان، محمد مصطفي. **حوكمة الشركات ودور أعضاء مجالس الإدارة والمديرين التنفيذيين**. دار الجامعة الإسكندرية. ط01، 2009. ص 14-15

[3]. بن عيسى، ريم. **تطبيق اليات حوكمة المؤسسات وأثرها على الأداء المالي دراسة حالة مؤسسات الجزائرية المدرجة في السوق الأوراق المالية**. مذكرة ماجستير علوم اقتصادية. كلية العلوم الاقتصادية التسيير والعلوم التجارية: تخصص اقتصاد وتسير المؤسسة. جامعة قاصدي مرباح، ورقلة، 2009. ص 14

أيضا تكمن أهمية حوكمة المؤسسات أيضا في توفير البيئة المناسبة لدعم فرص المؤسسات في الحصول على رأس المال والتمويل، فاهتمام المستثمرين بحوكمة المؤسسات. طالما أن تلك المؤسسات تتفوق على نظيرتها من ناحية الأداء المؤسسي كونها تعمل ضمن إطار الشفافة يؤدي الى حماية حقوق شركائها أكثرية كانوا أم أقلية، فيتوفر لديها عناصر جاذبة.[1]

حوكمة المؤسسات باعتبارها منهج يشمل جملة من الأنظمة والضوابط تهدف أساسا إلى التسيير الحسن للشركة والرقابة المترتبة عن ذلك التي تمارسها هياكلها المتمثلة في مجلس الإدارة، تكتسي أهمية كبيرة بالنسبة للمؤسسة ممثلة في التقليل من الفساد. ونتيجة لذلك جعل المستثمرين يقبلون على إستثمار أموالهم دون قيود تخوف من أي طارئ سيؤدي حتما إلى تراجعهم عن فكرة الاستثمار، وبالتالي عدم تمويل كافة المشاريع المختلفة. بالإضافة إلى التأطير التنظيمي للعلاقات التي تنشأ بين كل المساهمين والشركات من خلال إدراج نظام تحفيزي لأعضاء المجلس.[2]

تسعى قواعد وضوابط حوكمة المؤسسات إلى تحقيق مجموعة من الأهداف يمكن تلخيص أهمها فيما يلي:

- تعزيز قدرة المؤسسات على تحقيق أهدافها من خلال تحسين الصورة الذهنية والإنطباع الإيجابي عنها.
- تطوير عملية صنع القرار في المؤسسات بزيادة إحساس المديرين بالمسؤولية.
- رفع خاصية مصداقية البيانات والمعلومات وتحقيق سهولة فهمها عبر الحدود.
- تحسين درجات الشفافية والوضوح والإفصاح ونشر البيانات والمعلومات.
- إدخال اعتبارات القضايا البيئية والأخلاقية في منظومة صنع القرار.
- زيادة قدرة المشروعات على تحسين موقفها التنافسي وجذب استثمارات ورؤوس أموال أخرى.
- زيادة قدرة الإدارة على تحفيز العاملين وتحسين معدلات دوران العمالة واستقرار العاملين.
- تحقيق الاستقرار ومصداقية للقطاعات المالية على المستوى المحلي والدولي.[3]

---

[1]. بن عيسى، ريم. **المرجع السابق**. ص 15

[2] . بن قايد علي، محمد لمين. **حوكمة الشركات: نظام جديد للإدارة والرقابة**. مجلة البحوث في الحقوق والعلوم السياسية. المجلد، 08. العدد،01، 2002. ص 652

[3]. بن زغده، حبيبة. **دور الحوكمة المؤسسية في تعزيز واستدامة نمو المؤسسات دراسة حالة بعض المؤسسات الاقتصادية من ولاية جيجل**. أطروحة دكتوراه. كلية العلوم الاقتصادية والتجارية وعلوم التسيير: تخصص أعمال والتنمية المستدامة. جامعة سطيف 1، 2019. ص 34_35

- تدعيم عنصر الشفافية في كافة المعاملات وعمليات المؤسسات وإجراءات المحاسبة.
- تنمية المدخرات وتشجيع التدفقات مما يؤدي لتنمية الاستثمارات الإنتاجية ووصولا لتعظيم الأرباح وبعيد عن الاحتكارات.
- المراجعة المالية بشكل الذي يمكن من ضبط العناصر الفساد في أي مرحلة[1].

تعتبر مبادئ الحوكمة المؤسسية العمود الفقري لموضوع حوكمة المعلومات بشكل عام، فيظهر هذا جليا من خلال الإهتمام المتزايد بهذا الموضوع على مستوى المؤسسات والتنظيمات ذات الصلة، وبالتالي فإن هذه المبادئ تعددت حسب المنظمة التي قامت بإصدارها.شهر أبريل عام 1988؛ طلب المجلس منظمة التعاون الاقتصادي والتنمية من المنظمة أن تقوم بالإشتراك مع الحكومات الوطنية وغيرها من منظمات الدولية والقطاع الخاص بوضع مجموعة من المبادئ والإرشادات الخاصة بحوكمة المؤسسات.شهرماي 1999تم إصدار هذه المبادئ. وبعد التعديلات التي صدرت بنتيجة العديد من المشاورات العامة والمكثفة في أبريل 2004 أعتبرت تلك المبادئ هي الأساس الذي تستند إإليها الدول والمؤسسات عند قيامها بوضع الأسس المناسبة لتطبيق مفهوم حوكمة المؤسسات،[2] وكانت على النحو التالي:

1.حقوق المساهمين: يتضمن هذا المبدأ مجموعة من الحقوق التي تضمن الملكية الآمنة للأسهم، والإفصاح التام عن المعلومات، وحقوق التصويت، والمشاركة في قرارات بيع أو تعديل أصول المؤسسة بما في ذلك عمليات الإندماج وإصدار أسهم جديدة.[3]

2.المعاملة المتكافئة للمساهمين: يجب أن يكفل إطار حوكمة المؤسسات المعاملة المتكافئة لجميع المساهمين، ومن بينهم صغار المساهمين والأجانب منهم. كما سنبغي أن تتاح لكافة المساهمين فرصة الحصول على تعويض فعلي في حالة انتهاك حقوقهم.[4]

---

[1]. بن زغده، حبيبة. **المرجع السابق**.ص 34

[2]. البشير بن عمر محمد، ودادن عبد الغني. **نفس المرجع السابق**. ص 33

[3] . محمد مصطفي، سليمان. **حوكمة لشركات ودور أعضاء مجالس الإدارة والمديرين التنفيذيين**. دار الجامعة الإسكندرية. ط 01، 2009. ص 42_43

[4] . شنافة، جهرة؛ زرقاطة، مريم. **واقع حوكمة الشركات وسبل ارسائها في بيئة الأعمالالعربية**. مجلة مينا للدارسات الاقتصادية. المجلد، 02. العدد، 01، 2019. ص 57

3.دور أصحاب المصالح في حوكمة المؤسسات: يجب أن يضم إطار حوكمة المؤسسات الاعتراف بحقوق أصحاب المصلحة كما يوضحها القانون، وأن يعمل على تشجيع الإتصال بين المؤسسات وبين أصحاب المصالح لفتح فرص العمل وتحقيق الإستدامة للمشروعات القائمة على أسس مالية سليمة.[1]

4.الإفصاح والشفافية: ينبغي أن تكفل الحوكمة تحقيق الإفصاح الدقيق وفي الوقت الملائم بشأن كافة المسائل المتصلة بتأسيس الشركة ومن بينها الموقف المالي والأداء والملكية وأسلوب ممارسة السلطة.[2]

5.مسؤوليات مجلس الإدارة: يجب أن يتيح إطار حوكمة المؤسسات الخطوط الإرشادية الإستراتيجية لتوجيه المؤسسات .كما يجب أن يكفل المتابعة الفعالة للإدارة التنفيذية من قبل مجلس الإدارة، وأن تتم المساءلة من قبل مجلس الإدارة والمساهمين. وفي هذا السياق يضطلع مجلس الإدارة الشركة بالمهام التالية:

- تعيين أو إبعاد كبار المسؤولين في المؤسسة المعنيين بالإشراف على المهام المؤسسة وخططها الخاصة.
- صياغة ورسم إستراتيجية المؤسسة ومراجعتها وإعداد الخطط الرئيسية المتعلقة بالموازنات السنوية. وخطط العمل وسياسة المخاطر، وأهداف الأداء، ومراقبة أداء المؤسسة.
- مراقبة وإدارة تضارب المصالح بين كافة المعنيين بالمؤسسة بما في ذلك سوء إستخدام موارد المؤسسة.
- ضرورة توفير الأسس اللازمة لتفعيل إطار حوكمة المؤسسات من أجل رفع مستوى الشفافية وأن يتوافق هيكل الحوكمة مع الإطار القانوني ويحدد مسؤوليات الهيئات المختلفة خصوصا المسؤولة عن الإشراف والرقابة[3].

3.2.1.2 حوكمة إدارة السجلات :

يعتبر الجمعية الدولية المتخصصة في الوثائق والبيانات والمعلومات ARMA أن نظام إدارة السجلات أساس حوكمة المعلومات، فهو نظام إستراتيجي للتعامل مع الوثائق والمعلومات بصفة عامة وهو يجسد فعليا ما نسميه بالمقاربة العملية لحوكمة إدارة الوثائقية والمعلومات.[4]

---

[1] . شنافة جهرة، زرقاطة مريم. **المرجع نفسه**. ص 59

[2]. بن قايد علي، محمد لمين. **نفس المرجع السابق**. ص 651

[3]. خليل، محمد. **دور المحاسب الإداري في إطار حوكمة الشركات**. مجلة الدراسات والبحوث التجارية. المجلد، 01. العدد، 02، 2003. ص 33_34

[4] . مراد، كريم. خالد، شيروف. **نظام الأرشفة الإلكترونية SAE قراءة تحليلية في المصطلح والمفهوم**. مجلة المقدمة للدراسات الإنسانية والاجتماعية. المجلد، 07. العدد، 01، 2022. ص 116

وقد ظهرت إدارة السجلات لأول مرة في الولايات المتحدة الأمريكية في أواخر القرن التاسع عشر كحل لمشكل النقص الفادح الذي ظهر على مستوى التحكم في الوثائق اللازمة للتسيير الأمثل للإدارة الأمريكية بعد الإنتاج المتزايد للوثائق.[1]

ويعرف نظام إدارة السجلات بأنه نظام يهدف إلى:

- التكفل التام والكامل بالوثائق الإدارية منذ نشأتها حتى تطبيق مصيرها النهائي مرورا بعملية إنشاء الوثائق وإدماجها داخل النظام وتصنيفها، وتوفير شروط حفظها وتبليغها، بالإضافة إلى تسجيل مختلف العمليات المطبقة على هذه السجلات.
- تنظيم وتسيير السجلات مهما كان شكله، والوعاء الذي ثبتت عليه، أنشئت أو أستقبلت من طرف أي مؤسسة عمومية كانت أو خاصة في إطار ممارستها لمختلف نشاطاتها الإدارة اليومية، أو أي شخص طبيعي مسؤول عن إنشاء أو حفظ الوثائق.
- تحديد مختلف المسؤوليات الواجب على المؤسسات إحترامها إزاء وثائقها وذلك بتحديد المبادئ والإجراءات الأنظمة والمناهج الواجب إتباعها لأدائها على أتم وجه.
- حماية المحتوى والخصوصية وتخفيف المخاطر وتوفير الأمن للسجلات والوثائق، ومنع تسرب المعلومات وإحتواء التكاليف.
- تحديد وتأكيد قواعد الحفظ والتخلص التي تحدد الوقت الذي ينبغي إعادة تقييم المحتوى والتخلص منه[2].

يمكن تحديد متطلبات تطبيق حوكمة السجلات في المؤسسات في أربع متطلبات أساسية وهي: [3]

1. المتطلب الإستراتيجي: ويتمثل في ضرورة وجود رؤية استراتيجية مستقبلية تتناسب مع موارد المؤسسة وامكانيتها.

2. المتطلب الأخلاقي: ويتمثل في ضرورة وجود قواعد أخلاقية، وضرورة نشر ثقافة حوكمة السجلات والوثائق ومبادئها من الشفافية والمساءلة وغيرها على جميع المستويات الإدارية بالمؤسسة.

---

[1] . مراد، كريم؛ خالد، شيروف. **المرجع السابق**. ص 117

[2]. Uttam, Acharya. **Records management in documentaliste**. Revues Science de l'information. Vol (46). N (02), 2009. P 28- 30

[3]. شيماء، خالد شعبان محمد. **حوكمة الوثائق والمعلومات في المؤسسة والمتطلبات اللازمة لتطبيقها**. المجلة المصرية لعلوم المعلومات. المجلد، 11. العدد، 02، 2024. ص123

3. المتطلب الرقابي: ويتحقق من خلال الدعم وتفعيل الرقابة على المستويين الداخلي والخارجي للمؤسسة.[1]

4. المتطلب الإشرافي: ويتم من خلال دعم وتفعيل الدور الشرافي لجميع القيادات الإدارية ذات العلاقة والمسؤولية بالمؤسسة.[2]

5. المتطلب القانوني: تتطلب حوكمة السجلات نصوصا قانونية واضحة تعبر عن التوقعات والمسؤوليات، ويجب أن تبين السياسات والقوانين والسياسات بوضوح الأدوار والمسؤوليات لكل من مؤسسة والعاملين فيها. لذلك من الضروري وجود أدلة إرشادية ومدونات تحتوي على مجموعة من القيم والمبادئ والمعايير للسلوك المرغوب فيه والتي ترشد صناع القرارات والأنظمة لإجراءات المؤسسة بطريقة تحافظ على مصالح العاملين الأساسين وتحترم حقوق الجميع.[3]

6. متطلبات تنظيمية: تعني وجود إستراتيجية واضحة، حيث يعد وضع الإستراتيجيات من أهم الأدوار التي تقوم بها المؤسسات نحو الإدارة الوثائق والسجلات لأنها الركيزة الأساسية، والمفتاح الأساسي للقدرة التنافسية الإدارية والإقتصادية وللتنمية الشاملة. ولأن تطوير القوانين يتم في ضوء هذه الإستراتيجيات والقرارات الإستراتيجية في الإدارة يتم إتخاذها في ضوء التخطيط الفعال، ذلك يقتضي بالإلتزام بمبادئ حوكمة السجلات في صياغة إستراتيجية واضحة على المدى الطويل ونشرها بين العاملين في مختلف المستويات الإدارية.[4]

7. متطلبات إدارية: لا يمكن لحوكمة السجلات أن تنجح دون وجود القيادات الإدارية الفعالة التي تتبنى أهداف المؤسسة وتكون قادرة على فهمها وتنفيذها بالشكل الصحيح، كما أن السلطة في حوكمة السجلات لا تنشأ من السلطة القانونية للمؤسسة فقط، بل من القدرة على إستخدام هذه السلطة، لذلك من الضروري وجود قيادات إدارية فعالة في حوكمة السجلات كضرورة لتجنب الإجراءات القانونية للعاملين على حوكمة السجلات والوثائق بالمؤسسة.[5]

---

[1] . شيماء، خالد شعبان محمد. **المرجع نفسه**. ص 123

[2]. الزميتي، أحمد فاروقعلي. **واقع تطبيق مبادئ الحوكمة بجامعة العريش**. مجلة كلية التربية. المجلد،25. العدد، 25، 2019.ص 28

[3]. شيماء، خالد شعبان محمد. **المرجع السابق**. ص 124

[4] . ترار، عبد الكريم. شيهاب، أنفال. **الاطلاع على الوثائق الإدارية في ظل الحماية القانونية**. مجلة علم المكتبات. المجلد، 14. العدد، 01، 2022.ص 10

[5] . صعصاع البديري، إسماعيل؛ عمار حنين، منصر. **دور الإدارة في الحفاظ على الوثائق في التشريع العراقي**. مجلة بابل للعلوم الإنسانية. المجلد، 28. العدد، 02، 2020. ص 30

4.2.1.2 حوكمة أمن المعلومات:

أدت الزيادة السريعة في إستخدام التقنية والإنترنت خلال العقدين الأخيرين إلى الدخول لنحو مجتمع المعلومات، وأصبحت المنظمات تعتمد على أنظمة المعلومات الإلكترونية في تنفيذ المهام والوظائف المنوطة بها، ومن أهم تلكُ الأنظمة نظم المعلومات المحاسبية الإلكترونية؛ والتي تمثل نتائجها نقطة الإتصال بين المنظمة والأطراف ذات العلاقة. وتواجه نظم المعلومات المحاسبية الإلكترونية مخاطر كبيرة يمكن أن تستغل نقاط الضعف وثغرات، وأشارت إحدى الدراسات أن قيمة أعمال الجريمة الإلكترونية أصبحت تقدر بحوالي 105 بمليون دولار سنويا، وهذا الرقم يفوق قيمة أعمال تجارة المخدرات في جميع أنحاء العالم.[1]

وفي هذا السياق تؤثر مخاطر أمن المعلومات سلبا على المنظمات وعملياتها وأصولها والعاملين بها، بالإضافة إلى أن حدوث تلك المخاطر قد يؤدى إلى انخفاض القيمة السوقية للمنظمة؛ حيث تهدد سرية ونزاهة ومدى توافر المعلومات المحاسبية التي يتم معالجتها وتخزينها وإرسالها أو الإفصاح عنها بواسطة نظم المعلومات المحاسبية الإلكترونية. ولذلك لجأت العديد من المنظمات إلى تطبيق حوكمة أمن المعلومات، التي تهدف إلى حماية الأصول الإلكترونية من مختلف المخاطر المحتملة، من خلال إستخدام مجموعة من المعايير الدولية والتي يتم إستخدامها على نطاق واسع للتأكد من الوصول إلى مستوى الأمن المطلوب والكافي.[2]

وتعد حوكمة أمن المعلومات عنصر أساسيا من عناصر حوكمة الشركات، وتعرف بأنها ترتيب إستراتيجي لأمن المعلومات من خلال رقابة فعالة لإستخدام تقنية المعلومات وتحقيق المساءلة، وإدارة الأداء، وإدارة المخاطر؛ يتكون من القيادة والهياكل التنظيمية والعمليات المشاركة في حماية الأصول المعلوماتية، بهدف توفير بيئة رقابية مناسبة للحفاظ على حماية المعلومات من مختلف التهديدات، ودعم العمليات والنظم الخاصة بها والمخاطر المحتملة،و تحديد صلاحية صنع القرار وإطار المساءلة للتشجيع على سلوك مرغوب فيه للإستخدام تقنية المعلومات.وحسب منظمة التقييس العالمي ISO ووفق ما جاء في معيار Iso 27000 فإن أمن المعلومات يشير إلى الحفاظ على السرية، وسلامة توافر المعلومات.[3]

---

[1]. أبو موسى، عبد السلام أحمد. **مخاطر أمن نظم المعلومات المحاسبية الإليكترونية دراسة ميدانية على المنشآت السعودية.** مجلة الإدارة العامة. المجلد، 44. العدد، 03، 2004. ص 511_511

[2]. أبو موسى، عبد السلام أحمد. **المرجع نفسه.** ص512

[3] . مسوس، كمال. **ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الالكترونية.** المجلة الجزائرية للعولمة والسياسات الاقتصادية. المجلد،13، 2022. ص101

وتبرز أهمية حوكمة أمن المعلومات في العديد من المنافع للمؤسسات التي تقوم بتطبيقها، وتتمثل أهم تلك المنافع بما يأتي:

- تحديد المخاطر المتعلقة بأمن المعلومات والعمل على تخفيضها إلى مستويات مقبولة.
- الحماية من المساءلة المدنية أو القانونية؛ الناتجة عن عدم دقة المعلومات أو عدم بذل العناية الواجبة.
- تحسين وتعزيز تخصيص الموارد الأمنية المحدودة.
- ضمان وضع سياسة فعالة لأمن المعلومات، والالتزام بتلك السياسة.
- إدارة المخاطر بكفاءة وفعالية، وتحسين العمليات.
- الاستجابة السريعة للحوادث المتعلقة بأمن المعلومات.
- توفير مستوى من التأكيد على أن اتخاذ القرارات الحاسمة والهامة التي يستند على معلومات غير صحيحة ومضللة[1].

تتحددإستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية أو على مستوى الآداء وأيضا أهداف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها:

- التأكد من سرية وموثوقية المعلومات فلا يسمح للأشخاص الغير مخولين بالإطلاع عليها.
- ضمان صحة المعلومات ولم يتم تعديله أو العبث به.
- التأكد من استمرار عمل التكنولوجيا المعلومات والقدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله اليها.
- عدم انكار التصرف المرتبط بالمعلومات بحيث توفر القدرة على إثبات أن تصرفا ما قد تم من شخص ما في وقت معين[2].

وفي هذا الإطار يمكن تصنيف التهديدات التي تتعرض إليها المعلومات بصفة عامة إلى ما يلي:

1.تهديدات طبيعية: وهي الكوارث التي لا دخل للإنسان والأجهزة فيها؛كالفيضانات والزلازل والحرائق والصواعق وموجات الغبار التي تمس بأنظمة المعلومات وقد تؤدي إلى إنقطاع الخدمات الإلكترونية[3].

---

[1] . مسوس، كمال. **المرجع السابق**. ص107

[2] . قدايفة، أمينة. **استراتيجية أمن المعلومات**. مجلة أبعاد اقتصادية. المجلد، 06. العدد، 01، 2016.ص 166

[3]. بوضياف، سهيلة؛ حمراني، أمنة. **أمن المعلومات في الجزائر: الإجراءات والتحديات**. مجلة الجزائرية للأمن والتنمية. المجلد، 09. العدد، 16، 2020. ص 181

2.تهديدات بشرية: وهي التهديدات الناجمة عن العمال الذي يشتغلون في المؤسسات، حيث يتسببون في إختراق أمن المعلومات وقد تكون التهديدات البشرية داخلية من خلال إختراقها لخدمة مصالح معينة، أو الإفشاء ببعض أسرار المعلومة ككلمات المرور مثلا .تكون التهديدات البشرية عن قصد أو بغير قصد، أما التهديدات الخارجية تحدث من أفراد خارج المؤسسة وتشمل تهديدات البرمجيات والأجهزة والمعلومات.

3.تهديدات تقنية وفنية: تتعدد طرق وآليات إنتهاك البنية التحتية لتكنولوجيا المعلوماتومنهم من يلجأ إلى تخريبها وتدميرها[1]، ولعلى أبرز التهديدات مايلي:

أ. **الجرائم المعلوماتية وأشكالها:** تعتبر الجرائم المعلوماتية التي تستخدم التقنيات الإلكترونية من الجرائم التي تتطلب إلمام خاص بتقنيات وبرمجيات الحاسب الآلي ونظم المعلومات. صاحب الفعل يعد مخالف للقواعد وأصول إستخدام تلك النظم وإستغلالها أو تزييفها أو تزويرها وذلك يكون منافيا لقواعد القانون.

ب. **الفيروسات:** تعتبر الفيروسات والبرامج الضارة من أهم أسباب إرتكاب الجرائم المعلوماتية أو الحاسوبية، وأكثرها انتشارا في الوقت الحاضر.تأخذ الفيروسات عدة أنواع وفي تطور مستمر، تعد أخطر مهدد للأمن المعلوماتي مثل: الفيروسات التشغيلBoot sector virus، فيروس الماكرو Makro virus، فيروس المخفي، فيروسات العتاد، الفيروسات المتحولة.[2]

ت. **البرمجيات الضارة:** وهي عبارة عن برنامج تتسبب في أضرار تتراوح بين الإزعاج إلى غاية فقد البيانات وأيضا سرقة الأموال، وهذا الأسلوب يحتوي على عدة تقنيات منها: حصان طروادة Hors troyen، برامج الدودة Worm، القنبلة الموقوتة Bomb.[3]

5.2.1.2 حوكمة البيانات :

تعد البيانات النفط الجديد للمؤسسات، وموردا هاما وأساسيا في إدارة أعمالها وتحقيق أهدافها، لما تتمتع به من مزايا وخصائص، وتتعدد أنواعها ومصادرها. ويظهر أثر البيانات في مجالات العلوم، والقطاع العام، والقطاع الحكومي وغيرها من المجالات والقطاعات الأخرى نظرا لأهميتها البالغة وقيمتها المتزايدة[4].

---

[1]. بوضياف، سهيلة؛ حمراني، أمنة. **المرجع السابق**. ص 181

[2]. شوابكة، محمد أمين. **جرائم الحاسوب والأنترنيت: الجريمة المعلوماتية**. دار الثقافة والنشر والتوزيع. عمان. ط،04، 2004. ص 238

[3] . شوابكة، محمد أمين. **المرجع نفسه**. ص 239

[4]. العبدلية، رقية بنت خلفان بن ناصر. **تطبيقات حوكمة البيانات في سلطنة عمان**.المؤتمر والمعرض السنوي السادس والعشرين حول:التقنيات الناشئة وتطويرها في المكتبات والمؤسسات المعلومات. جمعية المكتبات المتخصصة؛ فرح الخليج العربي: الكويت، 2023. ص 493- 504

حيث يتم يوميا إنتاج كميات هائلة من البيانات الرقمية المتغيرة والمتنوعة مع ظهور التقنيات الحديثة التي تعمل على توزيعها وتبادلها على نطاق أوسع. وأصبحت البيانات تمثل الوقود والمحرك الرئيسي للمنافسة بين المؤسسات من خلالإنشاء مخازن وقواعد بيانات بهدف التحكم فيها وإتخاذ القرارات الإدارية على المستوى الداخلي والخارجي للمؤسسة. وعليه حوكمة البيانات مجال بحث حديث الظهور جذب اهتمامكبير قي العديد من القطاعات، كما أنها تعتبر أكبر تحدي لموظفي تكنولوجيا المعلومات من خلال التحكم فيها من جهة وضمان حمايتها وأمنها من جهة أخرى.[1]

يمكن تعريف حوكمة البيانات Data Governance بأنها القواعد التي تحكم تخزين البيانات ومشاركتها وإستخدامها، ويمتد نفعها إلى الحكومات بمساعدتها في تسخير قوة البيانات، وكذلك المستفيدين بمنحهم درجة أكبر من الشفافية والتحكم في كيفية إستخدام المؤسسات لبياناتهم الشخصية. وفي بعض الأحيان ينظر الى حوكمة البيانات بوصفها عملية فنية تقع ضمن مسؤولية أقسام تكنولوجيا المعلومات وحدها، لكنها في الواقع تشمل المعايير التقنية والقيادة والثقافة المؤسسية والسياسات وتتطلب معالجتها رؤية أوسع ترتبط بإستراتيجية الحوكمة أو المؤسسة.[2]

1.5.2.1.2آليات تنفيذ حوكمة البيانات:

تستخدم المؤسسات مزيجمنآليات الحوكمة، تساعد هذه الأخيرة في تخطيط أنشطة وإدارة البيانات والتحكم فيها. تشتمل آليات الحوكمة على هياكل رسمية تربط بين الأعمال التجارية وتكنولوجيا المعلومات ووظائفها إدارة البيانات والعمليات والإجراءات الرسمية لصنع القرار والمراقبة والممارسات التي تدعم المشاركة الفعالة والتعاون بين أصحاب المصلحة، باتباع الأدبيات الخاصة بإدارة تكنولوجيا المعلومات فإننا تميز بين هذه الآليات كالآتي: [3]

أ.الآليات الهيكلية: تحدد آليات الحوكمة الهيكلية كل ما يتعلق بإعداد التقارير، هيئات الحوكمة، الأدوار والمسؤوليات،تشمل الهيئة: الفريق التنفيذين وقائد حوكمة المعلومات، ومالك البيانات، ومسؤول البيانات ومجلس

---

[1]. العبدلية، رقية بنت خلفان بن ناصر. **المرجع السابق**. ص 493- 504

[2]. بن عيدة، فوزية؛ بحوصي، رقية. **حوكمة البيانات في المؤسسات التعليم العالي: الآليات، والاستراتيجيات، العوائق**. المجلة المغاربية للمخطوطات. المجلد، 20. العدد، 01، 2024. ص161

[3]. محي الدين، زكريا. **أليات حوكمة المؤسسة العمومية الاقتصادية: حالة المؤسسة العمومية الاقتصادية الجزائرية**. أطروحة دكتوراه، كلية العلوم الاقتصادية: تخصص المالية والمحاسبة، جامعة عبد الحميد بن باديس. الجزائر، 2020. ص 58

حوكمة البيانات، ومكتب حوكمة البيانات ومنتجي البيانات، ومستهلك البيانات[1]. ولكل منها أدوار ومهام كالتالي:

1. الفريق التنفيذي: يوفر التوجيه الإستراتيجي وتحديد أولويات الأعمال والتمويل.
2. قائد حوكمة البيانات: هو المسؤول عن الإدارة اليومية لبرنامج إدارة البيانات يقدم إرشادات تتعلق بتصميم البيانات وتسليمها وصيانتها ويشرف على الامتثال لسياسات البيانات. كما يقوم بتنسيق المهام لمضيفي البيانات، وتقديم تقارير دورية عن أداء حوكمة البيانات.
3. مالك البيانات: غالبا ما يكون مديرين تنفيذيين ومسؤولين عن الأصول البيانات في وحدة أعمالهم، فهم ينقلون متطلبات ومخاطر بيانات واسعة النطاق.
4. مشرف البيانات: قادة أعمال أو خبراء متخصصون في الموضوع، ولديهم معرفة تفصيلية حول الأعمال التجارية والبيانات ويمكنهم ترجمة هذه المتطلبات إلى مواصفات فنية.
5. مضيف البيانات: هم خبراء متخصصون من مناطق عمل محددة.
6. مجلس حوكمة البيانات: هو هيئة حوكمة هرمية شاملة متعددة الوظائف يحدد الإتجاه الإستراتيجي لبرنامج إدارة البيانات بالكامل ويلائمه مع الأهداف التنظيمية، وعلى ذلك يقوم مجلس إدارة البيانات بمراقبة البرنامج بما في ذلك أنشطة التحسين المستمرة، يقوم هذا المكتب بإنشاء قنوات اتصال والتحضير للاجتماعات، وتنسيق حل المشكلات، وتثقيف أصحاب المصلحة.
7. منتج البيانات: ينشأ منتج البيانات، البيانات أو جمعها ويحافظ على البيانات التي تم إنشاءها الأخرون.
8. مستهلك البيانات: هو مستخدم البيانات، حيث يقوم بتحديد المتطلبات والابلاغ عن المشكلات المتعلقة بالبيانات[2].

ب.الآليات الإجرائية: تهدف آليات الحوكمة الإجرائية إلى ضمان تسجيل البيانات بدقة وحفظها بشكل آمن وإستخدامها بفاعلية ومشاركتها بشكل مناسب وهي تشمل:

1. إستراتيجيات البيانات: تمثل مسار العمل رفيع المستوى يعتمد على أهداف العمل الإستراتيجي وهو يتألف من بيان الرؤية ودراسة الجدوى والمبادئ التوجيهية وغيرها والأهداف طويلة المدى وقصيرة المدىوخطة طريق التنفيذ.

---

[1]. Zeroual, Sihem. Tadjine, Farida. **Good Governance and development**: **A Critical Analysis of the Relationship**. Revue critique de droit et science politiques. Vu (03). Nu (02), 2019. P 178

[2]. Benkara Mostafa, Aicha. **Governance Of Personal Data Privacy in Algerian Legislation**. Revue Comparative legal studies. Vu (09). Nu (02), 2024. P 213

2. المعايير: تضمن معايير البيانات قابلية التشغيل البيئي داخل المنظمات وملائمة البيانات للغرض المطلوب، ويتم تحديد المعايير داخليا بواسطة مضيفي البيانات ومهندسي البيانات أو خارجيا بواسطة منظمات التقييس أو التقيين مثل Iso.
3. العمليات: تعتبر عمليات البيانات عنصر أساسيا في التنفيذ الناجح للحوكمة البيانات، وهي طرق موحدة وموثوقة وقابلة للتكرار تستخدم في إدارة البيانات. ومن الأمثلة على ذلك عمليات تطوير وصيانة قواعد معالجة البيانات. بالإضافة إلى نمذجة وتوثيق دورة حياة البيانات، صنع القرار وقياس الأداء وحل المشكلات[1].
4. الإجراءات: هي أساليب وتقنيات وخطوات موثقة لإنجاز مهمة أو نشاط معين تمتد على نطاق واسع عبر المؤسسات والشركات، على سبيل المثال: تصف إجراءات كيفية تحديد المسؤوليات وحقوق إتخاذ القرار أو تطوير نموذج بيانات أو تحديد أخطاء البيانات وحلها.[2]
5. الاتفاقيات التعاقدية: تتطلب إعدادات توفير البيانات ومشاركتها إتفاقيات تعاقدية بين الإدارات الداخلية المشاركة أو المنظمات الخارجية. ومن الأمثلة على هذه الاتفاقيات؛ إتفاقيات على مستوى الخدمة واتفاقيات مشاركة البيانات، يحدد تقييم التأثير الاجتماعي، ويحدد قانون الخدمات الرقمية DSA الجوانب القانونية وجوانب حوكمة البيانات.[3]
6. قياس الأداء: يهدف إلى تقييم فعالية إدارة البيانات عن طريق قياس مستوى تحقيق الهدف، تستند مقاييس الأداء على مستوى الشركة الى أهداف العمل الاستراتيجية مثل نمو الواردات وزيادة الربحية وتوفير التكاليف. كما تستند على المستوى المتوسط إلى أهداف الأعمال التشغيلية أو أهداف مجال القرار المحددة، وكلاهما مشتق من أهداف الأعمال الإستراتيجية على مستوى الشركة أو المؤسسة، تركز مقاييس الأداء على مستوى البرنامج على التقدم المحرز وتأثير برنامج إدارة البيانات.[4]
7. مراقبة الإمتثال: تهدف إلى تتبع وفرض التوافق مع المتطلبات التنظيمية والسياسات التنظيمية والمعايير والإجراءات وإتفاقيات مستوى الخدمة، وهذا يشمل الإشراف على متخصص البيانات، والاشراف على مشاريع وخدمات إدارة البيانات كما تشمل مراقبة الامتثال والتدقيق الذي يهدف الى تزويد أصحاب

---

[1] . محي الدين، زكريا. **المرجع السابق**. ص 61_62

[2] . الميلبي، أروى النصار؛ الضحوي، هناء علي. **نضج إدارة البيانات الرئيسية في المؤسسات الحكومية: دراسة حالة لوزارة النقل والخدمات اللوجستية**. مجلة دراسات المعلومات والتكنولوجيا. المجلد، 01. العدد،03، 2023. ص 07

[3] . الميلبي، أروى النصار؛الضحوي، هناء علي.**المرجع نفسه**. ص 10

[4] . زياني، زهرة. بودية، فاطمة الزهراء. **تقييم الأداء في المؤسسات الخدمية باستخدام تحليل البيانات المغلفة: جامعة الشلف نموذجا**. مجلة بحوث الإدارة والاقتصاد. المجلد، 01. العدد، 02، 2019. ص76

المصلحة بتقييمات موضوعية وغير حيازيه وتوصيات للتحسين، بناءا على نتيجة التدقيق. يمكن للشركات اتخاذ إجراءات تصحيحية ووقائية.[1]

8. إدارة المخاطر: تهدف إلى تحديد وإدارة وحل المشكلات المتعلقة بالبيانات وهي تشمل عمليات، لتوحيد قضايا البيانات وحل المشكلات، وتحديد الأشخاص المسؤولين عن المشكلات. بالإضافة إلى ذلك تساعد عملية التصعيد في معالجة المشكلات لتقديم الملاحظات والعمل على حللها حسب الأولويات القصوى، الهدف من إدارة المخاطر هو العمل على منع حدوث خطأ وإتباع أفضل الوسائل من شأنها حماية البيانات من الإتلاف أو القرصنة الإلكترونية كالتأمين، فضلا على هذا وضع سياسات وإجراءات كفيلة بمواجهة الخطر من أجل تقليل الخسائر التي تنتج أثناء حدوث الخطر.

ث. الآليات العلائقية: آليات الحوكمة العلائقية تسهل التعاون مع أصحاب المصلحة وهي تشمل ما يلي:

1.الاتصال: يهدف الإتصال إلى زيادة الوعي ببرامج إدارة البيانات بشكل مستمر وأصحاب المصلحة، فخلق الوعي هو خطوة أساسية في إرساء الالتزام المشترك، وضمان التأييد والمشاركة الفعالة لأصحاب المصلحة والقضاء على مقاومة التغيرات المطلوبة، يمكن أن تساعد خطة الاتصال من خلال تحديد أصحاب المصلحة وقنوات الاتصال وأدوات الدعم والمبادرات للاحتفاظ بالالتزام.

2. التدريب: تضمن برامج التدريب أن أصحاب المصلحة لديهم تلك المعرفة والتعليمات اللازمة لدعم تنفيذ حوكمة البيانات بالإضافة الى ذلك يساعدهم التدريب المستمر على التصرف وفقا لسياسات البيانات والعمليات والإجراءات ويمكن اجراء التدريب في شكل تدريب قائم على الكمبيوتر، وتدريب في الفصول الدراسية، وتدريب خاص بالوظيفة والمتعلقة بالمشروع وثقافة التدريب الفردية تقدر أصول البيانات[2].

3.تنسيق صنع القرار: يصف تنسيق صنع القرار الممارسات الخاصة بالموائمة بين الوظائف، يتميز النهج الهرمي بهيكل شبيه بالهرم مع الوجود سلطة إتخاذ القرار في المستوى الأعلى[3]، وتشمل العناصر الرئيسية للنهج الهرمي التوجيه والتحكم، حيث يستفيد النهج التعاوني من السلوك التعاوني لتوضيح الاختلافات وحل المشكلات، ويستخدم اليات التنسيق الرسمية مثل مجموعات العمل واللجان وفرق العمل وأدوار التكامل، ولكن أيضا اليات

---

[1] . زياني، زهرة. بودية، فاطمة الزهراء. **المرجع نفسه**.ص76

[2] . إبراهيم، نرمين. **حوكمة البيانات والوثائق في إدارة جامعة الإسكندرية العامة**. المجلة العلمية للمكتبات والوثائق والمعلومات. المجلد، 04. العدد، 10، 2021. ص 266 _ 267

[3] . إبراهيم، نرمين. **حوكمة البيانات والوثائق في إدارة جامعة الإسكندرية العامة**. المجلة العلمية للمكتبات والوثائق والمعلومات. المجلد، 04. العدد، 10، 2021. ص 266 _ 267

التنسيق غير الرسمية مثل الأحداث المشتركة بين الإدارات ومراجعات الأداء عبر وحدات العمل والتناوب الوظيفي.[1]

من خلال ما سبق ذكره، نخلص أن حوكمة البيانات جزء هام في منظومة المؤسسة سواء ربحية أو غير ربحية، حيث تمثل البيانات محرك أساسي لنجاحها أو فشلها. وتظهرأهداف حوكمة البيانات في مايلي:

- نشر ثقافة مشاركة البيانات والتعاون لتعزيز وتطوير البيانات والمعلومات والأصول المعرفية.
- تحقيق التكامل بين الجهات الحكومية.
- تمكين الجهات الحكومية من إعادة سياستها وتنفيذ خططها والقيام بإشراف المستقبل.
- المحافظة على خصوصية البيانات الشخصية، وسرية البيانات الحساسية.
- تعزيز مفهوم وممارسات البيانات المفتوحة لتحسين الشفافية لدى الجهات العامة وتشجيع البحث والابتكار ودفع النمو الاقتصادي.
- تعزيز الشفافية وإرساء قواعد الحوكمة عن طريق توزيع الأدوار والمسؤوليات.
- رفع مستوى الثقة في الخدمات المعتمدة على البيانات.
- تمكين الجهات من الاستثمار والابتكار في الخدمات المعتمدة على البيانات الشخصية لتعزيز المكاسب التنموية والاقتصادية والتنافسية مما يساهم بشكل إيجابي في رفع الناتج الإجمالي المحلي[2].

6.2.1.2 حوكمة نظم المعلومات:

في ظل الثورة المعلوماتية التي يتسم بها العصر الحديث والحاجة الملحة للحصول على المعلومات سواء للفرد أو المؤسسة، وتوجه المؤسسات نحو الحوسبةظهرت نظم المعلومات. ولقد وردت العديد من المفاهيم المتعلقة بنظم المعلومات، وهي كالآتي:

تعرف نظم المعلومات حسب LAUDONبأنها:" مجموعة من العناصر المترابطة المادية والبشرية والبرمجيات تعمل على جمع ومعالجة وتخزين وإسترجاع المعلومات وتوزيعها بهدف دعم إتخاذ القرارات داخل المؤسسة، كما تساعد المسيرين والعاملين في كسب وإبتكار معرفة جديدة وحل المشكلات وإبداع منتجات وخدمات وطرائق وعمليات جديدة".[3]

---

[1] . إبراهيم، نرمين. **المرجع نفسه**. ص 288

[2] . قوت، سهام. **إدارة البيانات الضخمة في الشركات التقنية: دراسة حالة شركتي google وMeta**. مجلة دراسات وأبحاث. المجلد، 15. العدد، 03، 2023. ص 63

[3]. مسوس، كمال؛ حديد، نوفيل. **العلاقة بين حوكمة نظم المعلومات وحوكمة المؤسسات وسيرورة تطبيقها بمؤسسات التعليمالعالي**. المجلة الجزائرية للعولمة والسياسات الاقتصادية. المجلد، 05. العدد، 01، 2014. ص 123

كما يعرف أيضا بأنه"نظام منهجي محوسب قادر على تكامل البيانات من مصادر مختلفة بقصد توفير المعلومات الضرورية للمستخدمين ذوي الاحتياجات المتشابهة. أي أنه نظام مخصص للحصول على صاغة وتكييف ومعالجة البيانات كمعلومات وتقديمها للمديرين عندما يحتاجونها."[1]

أصبح الاستغناء عن حوكمة نظم المعلومات في المؤسسة اليوم مستحيل. هناك العديد من الأسباب تجعل الاستعانة بحوكمة أنظمة المعلومات لا مفر منها من بين أهم هذه الأسباب ما يلي:

- المشكلة الإدارية: إن جوهر المشكلة الإدارية يتمثل باختصار في إتخاذ القرارات التي تحدد كيفية توزيع الموارد المحدودة على أوجه الإستخدام غير المحدودة، بحيث تؤثر العوامل الخارجية التي لا تملك الإدارة السليمة قدرة السيطرة عليها إلا في حدود التخفيف من آثارها السلبية. كما أن تلك القرارات تتخذ في ظروف تتصف بنقص المعلومات وعدم التأكد وصعوبة الرؤية المستقبلية بصورة صحيحة واتخاذ القرارات السليمة.
- تقسيم العمل: كلما إزداد التقسيم الوظيفي المكاني للعمل كلما إزدادت أهمية التبادل المعلومات بين الإدارات المختلفة للمنظمة وبالتالي تنشأ الحاجة إلى نظام المعلومات ليؤمن تقديم المعلومات إلى المستويات الإدارية المختلفة في الوقت المناسب وبالشكل الملائم[2].
- التقدم التقني والعملي: إن التطورات العملية والتقنية للإنتاج تجعل العملية الإنتاجية أكثر تعقيدا، فالمشروعات كبيرة الحجم تحتاج إلى رؤوس أموال ضخمة. هذه العوامل أدت الى إزدياد مخاطر القرار[3]

بحيث أن أي قرار خاطئ قد يؤدي إلى خسارة كبيرة لأن الإجراءات الإنتاجية أكثر تعقيدا، وتحتاج إلى كم هائل من المعلومات التي يجب أن تتدفق بشكل منتظم بين المراكز الإدارية المتعددة في المنظمة.

- المنافسة الدولية المحلية: في ظل التنافس الموجود في السوق بين المنظمات على الصعيد الدولي والمحلي يتطلب بعض البيانات الهامة، كما أن ثورة الاتصالات تؤدي إلى تغير مستمر في أذواق المستهلكين مما يلقي على عاتق المنظمة أعباء متابعة أذواق المستهلكين ورغباتهم من أجل تطوير الإنتاج والخدمات بما يتلاءم مع التغيرات.[4]

---

[1] . سلطان، إبراهيم. **نظم المعلومات الإدارية: مدخل النظم. الدار الجامعية**. الإسكندرية. ط، 01، 2005. ص 01_02

[2]. شعباني، مجيد؛ مزوار، منوبة. **حوكمة نظم المعلومات كآلية لتدعيم الميزة التنافسية للمؤسسة**. مجلة العلوم التجارية. المجلد، 14. العدد، 02، 2015.ص25 _27

[3]. مسوس، كمال. **نحو حوكمة نظم المعلومات ونظم المعلومات الحديثة في مؤسسات التعليم العالي: دراسة حالة عينة من مؤسسات التعليم العالي**. أطروحة لنيل شهادة دكتوراه. كلية العلوم التجارية والاقتصادية وعلوم التسيير: تخصص العلوم الإدارية. جامعة إبراهيم سلطان شيبوط الجزائر 03. الجزائر، 2018. ص 100

[4]. مسوس، كمال. **المرجع نفسه**. ص 100

2.2مبررات إعتماد حوكمة المعلومات:

لقد حظيت مفهوم حوكمة المعلومات في الآونة الأخيرة بإهتمام متزايد من قبل العديد من الجهات، ولقد ساهمت في ذلك أسباب وعوامل مختلفة وهي كالآتي:

أ. العولمة والتغيرات ال: مع زيادة التبادل المعلوماتي عبر الحدود، خلقت بيئة معقدة تتطلب إدارة معلومات فعالة تهدف إلى تنظيم هذه المعلومات وضمان أمنها وحماية الخصوصية، ومع تزايد الإعتماد على البيانات في إتخاذ القرارات أصبح من الضروري وجود إطار عمل واضح لضمان جودة البيانات وإستخدامها المسؤول، حسب رواد الفكر في حوكمة المعلومات باركلي وبلير تم تحديد أسباب تفسر سبب ظهور مصطلح حوكمة المعلومات، وهي كالآتي:

- ❖ من الصواب تطبيق حوكمة المعلومات لأنها تساعد المؤسسات على التخلص من المعلومات غير الضرورية بطريقة مبررة، لذلك تحتاج المؤسسات إلى طريقة معقولة للتخلص من المعلومات بهدف تخفيض التكاليف والتخفيف من تعقيد بيئة تقنية المعلومات. إن وجود المعلومات الغير الضرورية يجعل الإستفادة من المعلومات القيمة أمرا صعبا ومكلفا.
- ❖ تطبيق حوكمة المعلومات لأن المؤسسات لا يمكنها التخلص من كل شيء بشكل عشوائي بل يجب التخلص من المعلومات المناسبة التي لم تعد ضرورية في المكان المناسب وفي الوقت المناسب وتقدم حوكمة المعلومات نظاما لاتخاذ قرارات رشيدة لتحديد أي المعلومات التي يجب الاحتفاظ بها[1].
- ❖ تخفض التكاليف وتخفف من العناء في الكشف عن الأدلة الالكترونية، ان إدارة المعلومات بشكل استباقي يقلل كمية المعلومات المعرضة للكشف مع الأدلة الالكترونية وتبسط مهمة العثور على المعلومات وتوليدها.
- ❖ تساعد حوكمة المعلومات عمال المعرفة في فصل "الإشارة" عن الضجيج في تدفقات المعلومات، من خلال مساعدة المؤسسات في التركيز عن المعلومات الأكثر قيمة حيث تقوم تقنية المعلومات بتحسين توصيل المعلومات وزيادة الإنتاجية.
- ❖ طريقة مثبتة كي تستجيب المؤسسات للقوانين والتقنيات الجديدة التي تخلق متطلبات وتحديات جديدة. ومع مرور الوقت لن تكون مشكلة حوكمة المعلومات صعبة الأمر الذي يحتم المؤسسات المباشرة بتطبيقها[2].

---

[1] . بن خضير، أحمد بن عبد الله. **المرجع السابق**. ص 35

[2] . Kaddouri, Ammar. **Op.cit**. P 35

❖ لابد أن تحدد المؤسساتالمخاطر والمعلومات بشكل دقيق، ويشكل إخفاق اؤسسة في إدارة مخاطر إدارة المعلومات خطرا كبيرا تعمل حوكمة المعلومات على التخفيف شدته بما يشمل ذلك المخاطر المالية والقانونية والإستراتيجية والأمنية.

فالإدارة السليمة للمخاطر تساعد المؤسسات على تحديد هذه المخاطر وإيجاد طرق لمعالجتها، تستخدم المؤسسات برنامج إدارة المؤسسة للتنبؤ بالمشاكل المحتملة وتقليل الخسائر. على سبيل المثال يمكنك استخدام تقييم المخاطر للعثور على ثغرات أمنية في نظام الكمبيوتر الخاص بك واصلاحها.[1]

3.2أدوار ومسؤوليات حوكمة المعلومات

تعتبر حوكمة المعلومات إطار إستراتيجي مهم في المؤسسةلما لها من دور كبير في دعم أهدافها ورؤيتهاوتتحدد أدوار حوكمة المعلومات في مايلي:

1.3.2الدور الإستراتيجي لحوكمة المعلومات:

1.1.3.2تحسين أقصى قيمة من أصول المعلومات :

أ.حماية الأصول: المعلومات تعتبر المعلومات عنصر مهم في المؤسسة، وحوكمة المعلومات تساعد في حمايتها من الضياع أو التلف والوصول الغير المصرح به. فالمعلومات هي رأس المال الفكري. فكما تحمي المؤسسات أصولها، بحفظ الأموال في البنوك وتوفير بيئة عمل امنة للموظفين فعليها أيضا حماية رؤوس أموالها الفكرية، ذلك أن الرأس المال الفكري في المؤسسة يشمل العديد من الأمور منها: براءات إختراع، والمعاملات والمعلومات التحليلية[2].

ومنع الخروقات الأمنية من الإرتفاع، وتزايد قراصنة الحاسوب في كل مكان. الأمر الذي أجبر المؤسسات على وضع تدابير أمنية قوية من أجل البقاء.[3]

ب.الإمتثال للقوانين واللوائح: العديد من الصناعات تخضع لقوانين ولوائح بشأن حماية البيانات والخصوصية وحوكمة المعلومات تساعد المؤسسات على الإمتثال للمتطلبات القانونية والتنظيمية التي تضعها المؤسسات، وكذلك على سياسات المؤسسة الداخلية من أجل حماية الخصوصية وإدارة المخاطر والنزاعات.[1]

---

[1]. Kaddouri, Ammar. **La relation des Risk management Et l'audit interne dans la Gouvernance des Epe.**Revue de recherche en finance et comptabilité. Vo (01). Nu (02),2016. P 35

[2] . بن الطيب، إبراهيم. **أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة.** مجلة التنمية والاقتصاد التطبيقي. المجلد، 02. العدد، 01، 2018. ص 34

[3] . بن الطيب، إبراهيم. **المرجع نفسه.** ص 34

ت.تحسين إتخاذ القرارات: من خلال توفير معلومات دقيقة وموثوقة في الوقت المناسب تساعد حوكمة المعلومات في إتخاذ قرارات أفضل على جميع المستويات في المنظمة.[2]

ث.توفر إطار عام عالي المستوى: تقدم هيكل عام وشامل للمؤسسة يحدد المسؤوليات والأدوار والمسارات التي يجب إتباعها في التعامل مع المعلومات، هذا الإطار يعمل كمرجع أساسي لجميع الموظفين في المؤسسة مما يضمن إتساق وتوحيد العمليات المتعلقة بالمعلومات.[3]

2.1.3.2 التوافق مع القوانين

أ. **الحد من المخاطر القانونية:** الامتثال للقوانين واللوائح يساعد في تجنب المخاطر القانونية والمالية مثل:

قوانين حماية البيانات: مثل قوانين الخصوصية العامة GDRP وقوانين حماية البيانات الأخرى التي تفرض قيودعلى جمع وإستخدام البيانات الشخصية[4].

ب.قوانين الملكية الفكرية: يمكن تقسيمها إلى الحقوق الملكية التي تحمي حقوق المؤلف والعلامات التجارية والاختراعات والنماذج الصناعية، وأيضا المعلومات السرية والتي تشمل الصيغ والأسرار التجارية والقواعد البيانات وخطط العمل وغيرها من المعلومات التي تقدم للمنظمة ميزة تنافسية.

بناء الثقة مع أصحاب المصلحة من خلال حماية المعلومات الشخصية والسرية، وتبني المنظمة ثقة أكبر لدى عملائها وشركائها وموظفيها:[5]

ت. العملاء: حماية البيانات الشخصية للعملاء يزيد من ثقتهم بالشركة ويجعلهم أكثر استعدادلمشاركة معلوماتهم.

ث. الشركاء: حماية المعلومات التجارية المشتركة تبني علاقات قوية وطويلة الأمد مع الشركاء.

ج. الموظفون: حماية المعلومات الشخصية للموظفين تخلق بيئة العمل آمنة وموثوقة.

---

[1]. قاشي، يوسف؛ خلدون، زينب. **امتثال المصارف الإسلامية للمعايير الشرعية وأهميته في تفعيل الحوكمة وتحقيق السلامة المصرفية**. مجلة التنمية والاستشراف للبحوث والدراسات. المجلد، 02. العدد، 02، 2017. ص 28

[2]. غضبان، حسام الدين. **مساهمة في اقتراح نموذج لحوكمة المؤسسات الاقتصادية الجزائرية دراسة حالة مجموعة من المؤسسات الاقتصادية**. أطروحة لنيل شهادة دكتوراه. كلية العلوم الاقتصادية والتجارية وعلوم التسيير: تخصص تسيير منظمات. جامعة محمد خيضر. بسكرة، 2014. ص 20 _ 22

[3]. غضبان، حسام الدين. **المرجع نفسه**. ص 30

[4]. عباس، زهوى؛ بن عبيدة، نجوى. **التدقيق الداخلي كأحد أهم الآليات الداخلية لتجسيد مبادئ حوكمة الشركات**. مجلة بحوث متقدمة في الاقتصاد واستراتيجيات الأعمال. المجلد، 03. العدد، 01، 2022. ص 18 _ 20

[5]. عباس، زهوى؛ بن عبيدة، نجوى. **المرجع السابق**. ص 23

د.**المستثمرين**: حماية المعلومات المالية للشركة تجذب المستثمرين وتزيد من قيمة الشركة.

2.3.2 الدور التشغيلي لحوكمة المعلومات:

1. توفر حوكمة المعلومات نهجشاملا ومنهجيا لإدارة المعلومات يدعم عمليات المنظمة من خلال دمج إدارة المعلومات وأمن المعلومات والخصوصية، والإمتثال وإستمرارية الأعمال وإستعادة الكوارث والإكتشاف الإلكتروني وغيرها من الجوانب ذات الصلة بتوجيه المعلومات والتحكم فيها من أجل منع حدوث فجوات في إدارة المعلومات ويقلل من المخاطر المحتملة.[1]
2. تحدد ماهية المعلومات المؤسسية الموجودة ومكانها والإجراءات التي يمكن إتخاذهبشأنها وكيفية إدارتها والتحكم فيها مما ينتج عنه معلومات قيمة يمكن إستخدامها وإعادة إستخدامها مرات عديدة.فحوكمة المعلومات تساعد المؤسسة على فهم نوع البيانات التي تمتلكها، سواء كانت بيانات مالية أو بيانات عملاء أو بيانات عمليات أو أي نوع آخر من البيانات. هذا التحديد يساعد في تقييم قيمة هذه البيانات وكيف يمكن إستخدامها لتحقيق أهداف المؤسسة،فضلا على هذا نجد حوكمة المعلومات تمكننا من معرفة مكان تخزين البيانات سواء كانت على خوادم داخلية أو سحابة،وبالتالي معرفة مكان البيانات يساعد على حمايتها من الضياع أو الوصول غير المصرح به.[2]
3. تدعم التنظيم المنهجي لأصول المعلومات، مما يتيح زيادة التوافر والمشاركة والتعاون ويوفر بحثا واسترجاعأسرع للمعلومات مما يسهل الوصول إليها من قبل جميع الموظفين المعنيين، ويشجع ذلك على مشاركتها بين الموظفين، هذا يؤدي إلى تبادل الأفكار والمعرفة مما يعزز الابتكار وتحسين الأداء. فضلا على ذلك نجد أن التنظيم المنهجي يسهل التعاون بين مختلف الأقسام والموظفين، عندما يكون الجميع على دراية بمكان وجود المعلومات وكيفية الوصول اليها، يصبح من السهل العمل معا على المشاريع وتحقيق الأهداف المشتركة.[3]
4. تقليل التكاليف المرتبطة بالتخزين والموارد المطلوبة لإدارة المعلومات أو اكتشافها من خلال اعتماد برنامج للتخلص من المعلومات أو اكتشافها للقضاء على فقدان المعلومات التجارية. وهذا يحدث من خلال عدة طرق:[4]

---

[1]. خلفلاوي، شمسضيات. **مفهوم إدارة المعلومات ومنهجية عملها**. مجلة الحقوق والعلوم الإنسانية. المجلد، 05. العدد، 01، 2012. ص 127

[2]. بودحاح. عبد الجليل. **التوجه نحو إدارة نظم معلومات حديثة في المنشأة – مدخل نظري–**. المجلة الجزائرية للدراسات المالية والمصرفية. المجلد، 02. العدد، 01، 2012. ص10 _ 15

[3]. غنيمات، رغد. **إدارة المعلومات والأرشفة الرقمية في المؤسسات الحكومية**. مجلة العربية للنشر العلمي. المجلد، 02. العدد، 41، 2022. ص 141

[4]. نعيمات، محمد خلود سليمان. **حذف الملفات المكررة والتخلص من البيانات والمعلومات المكررة**. المجلة العربية للنشر العلمي. المجلد، 02.. العدد، 50، 2022. ص 1477 _ 1484

- تحديد المعلومات التي لم تعد ذات قيمة أو ضرورية للمؤسسة، والتخلص منها بشكل آمنيقلل من حجم البيانات التي تحتاج إلى تخزينها وإدارتها وبالتالي يقلل من التكاليف المرتبطة بالتخزين.
- تساعد حوكمة المعلومات في تحديد المعلومات المفقودة أو الضائعة مما يمنع فقدان معلومات تجارية قيمة، هذا يقلل من الوقت والجهد المطلوبين لإعادة بناء المعلومات المفقودة وبالتالي بقلل من التكاليف.
- تنظيم المعلومات بشكل منهجي يسهل العثور على المعلومات بشكل منهجي والوصول إلى المعلومات المطلوبة بسرعة،ويقلل من الوقت والجهد المطلوبين للبحث عن المعلومات وأيضايرفع من إنتاجية الموظفين.

5. فهم وتنظيم المعلومات: تلعب حوكمة المعلومات دور كبير في فهم وتنظيم البيانات الشاملة، فهي التي توفر الإطار اللازم لضمان جودة البيانات وأمنها، مما يمكن المؤسسات من الاستفادة القصوى من البيانات في دعم عمليتها واتخاذ قراراتها. وفهم كيفية توزيع البيانات في المؤسسة بأكملها، وكميتها ومكان تواجدها. ومن يملكها و قيمتها، مع تحديد الهيكل العام للبيانات بما في ذلك العلاقات بين الجداول والكيانات، مما يسهل إسترجاع المعلومات وتحليلها وسهولة الوصول إليها، هذا الأمر الذي يحدد جودة البيانات وموثوقيتها.[1]
6. تخزين البيانات الوصفية: تخزين البيانات الوصفية في حوكمة المعلومات يساعد على تحديد موقع المعلومات وسهولة البحث والاسترجاع بشكل أسرع وأكثر دقة؛فإذا كنت تبحث عن جميع الصور المتعلقة بمنتج جديد يمكنك ببساطة البحث عن الكلمة المفتاحية "منتج جديد "[2].

بالإضافة أنها تساهم في الحفاظ على سياق البيانات وتاريخها. مع تطبيق إجراءات أمنية مناسبة لها. وبالتالي حوكمة المعلومات تلعب دورا حاسما في إدارة البيانات الوصفية مما يضمن جودتها واكتملها ودقتها، مما يؤدي الى تحسين عملية البحث عن البيانات واستخدامها، وحماية الأصول الرقمية للمؤسسة.[3]

7. إدارة التغيير: مواكبة الأشكال الجديدة للمحتوى والمتطلبات التجارية وحوكمتها، وبالتالي حوكمة المعلومات هي بمثابة البوصلة التي توجه المؤسسات في عالم البيانات المتزايد والمسؤولة عن إدارة التغيير والتأكد من أن المعلومات تتدفق بسلاسة وفعالية لتلبية احتياجات الأعمال المتجددة. وتحديد أفضل الطرق لتخزين وتحليل واستخدام المعلومات، وضمان جودتها وسلامتها. كما تعمل على مواكبة التطورات التكنولوجية المستمرة،

---

1. Chabani, Said. **Le Management de l'information Et la prise De Décisions En Entreprise**. La Revue de la communication et du journalisme. Vu (02). Nu (01), 2015. P 79

2. الخضر،أبو بكر سلطانمحمد. **الميتاداتا بمواقع قواعد بيانات الوصول الحر في مجال علم المعلومات والمكتبات: دراسة تحليلية تقويمية**. مجلة التكامل في البحوث العلوم الاجتماعية والرياضية. المجلد، 05. العدد، 02، 2021. ص 68

3. الخضر،أبو بكر سلطانمحمد. **المرجع نفسه**.ص 68

مثل ظهور أنواع جديدة من المحتوى، وتكييف الإجراءات لتناسب هذه التطورات من أجل التميز في عصر المعلومات.[1]

8. ضمان أمن البيانات والامتثال: فهي تعمل على وضع السياسات والإجراءات اللازمة لحماية البيانات من الاختراقات والوصول الغير المصرح به. كما تضمن حوكمة المعلومات أن يتم التعامل مع البيانات بشكل صحيح ووفقا لمتطلبات القانونية، مثل قوانين حماية البيانات الشخصية. من خلال حوكمة المعلومات، تستطيع المؤسسات بناء ثقافة أمنية قوية، مع تقليل المخاطر المحتملة، وتعزيز الثقة لدى العملاء والشركاء.[2] وذلك عن طريق:[3].

9. ادارة المحتوى: يتم تحديد سياسات للإنشاء المحتوى وتخزينه والتخلص منه.

10. التوعية والتثقيف: تدريب وتوعية الموظفين على أهمية الحوكمة الجيدة والامتثال للأنظمة والقوانين المتعلقة بالبيانات.

11. التقييم المستمر: تقوم حوكمة المعلومات بتقييم مدى التزام المنظمة بالأنظمة والقوانين بشكل مستمر، وتحديد أي نقاط ضعف وتصحيحها.

12. إدارة المخاطر: تساعد حوكمة المعلومات في تحديد المخاطر المحتملة بمعالجة البيانات، مما يسهل عملية التحقيق في أي حوادث أو انتهاكات[4].

4.2 أهداف حوكمة المعلومات:

1.4.2 تحسين جودة البيانات ودقتها.

---

1. EL Qasmi, Mohamed Jaouad. Kriouile, Abdelaziz. **Le Management de l'information** : **Une Dimension Stratégique Et Organisationnelle**. Revue de l'information scientifique et technique. Vu (14). Nu (01),2004. P 129

2. بن محمد، هدى؛ كورتل، نجاة. **المعايير الدولية لإدارة أمن المعلومات**. المجلد، 20. العدد،02، 2023. ص 179

3. بن محمد، هدى. كورتل، نجاة. **المرجع نفسه**. ص 180

4. بن محمد، هدى؛ كورتل، نجاة. **المرجع السابق**. ص 180

تُعد جودة البيانات من العوامل الأساسية التي تؤثر على كفاءة العمليات المؤسسية واتخاذ القرار داخل المؤسسات الأكاديمية والمكتبات الجامعية. فالمعلومات غير الدقيقة أو غير المكتملة قد تؤدي إلى أخطاء في التحليل، واتخاذ قرارات غير صائبة وهدر في الموارد. تسعى حوكمة المعلومات إلى وضع سياسات ومعايير صارمة لضمان دقة البيانات وموثوقيتها، مما يسهم في تحسين كفاءة الأنظمة التشغيلية وتعزيز الاستفادة من المعلومات المتاحة، ولتحقيق جودة البيانات.[1] وتعتمد حوكمة المعلومات على مجموعة من المعايير التي تشمل:

- الدقة (Accuracy): ضمان أن تكون البيانات صحيحة وخالية من الأخطاء أو المعلومات غير الدقيقة.
- الاكتمال (Completeness): التأكد من أن جميع المعلومات المطلوبة متاحة ولا توجد بيانات ناقصة تؤثر على دقة التحليل.
- التناسق (Consistency): ضمان تطابق البيانات عبر الأنظمة المختلفة بحيث لا تتعارض المعلومات مع بعضها.
- الحداثة (Timeliness): تحديث البيانات بانتظام لضمان أنها تعكس أحدث المعلومات المتاحة[2].
- الإمكانية (Accessibility): توفير البيانات بطريقة تتيح سهولة الوصول إليها من قبل المستخدمين المخولين بذلك[3].

2.4.2 تعزيز أمن المعلومات وحماية البيانات الحساسة في المؤسسات الأكاديمية.

مع تزايد التهديدات السيبرانية والهجمات الإلكترونية، أصبح تعزيز أمن المعلومات وحماية البيانات الحساسة أمرًا ضروريًا لضمان استمرارية العمل وحماية خصوصية المستخدمين. تسهم حوكمة المعلومات في وضع إستراتيجيات فعالة لحماية البيانات من الاختراقات، والتسريبات، والضياع غير المقصود، وذلك من خلال عدة تدابير رئيسية بداية يتم تحديد مستويات الوصول بحيث يُسمح فقط للأفراد المخولين بالاطلاع على المعلومات الحساسة، مما يقلل من مخاطر الوصول غير المصرح به.[4]

ومن ثم تلعب تقنيات التشفير دورًا مهمًا في حماية البيانات أثناء نقلها أو تخزينها، حيث يتم تحويل المعلومات إلى صيغة غير قابلة للقراءة إلا من قبل الأطراف المصرح لها، مما يعزز من سريتها. بالإضافة إلى ذلك، يتم تعزيز أنظمة

---

[1] . غنيمات، رغد. **المرجع السابق**. ص 139

[2] . بن زغده، حبيبة. **المرجع السابق**. ص 38

[3] . بن زغده، حبيبة. **المرجع نفسه**. ص 38

[4] . الخضر،أبو بكر سلطان محمد. **المرجع السابق**. ص 70

المصادقة مثل المصادقة متعددة العوامل (MFA)، التي تتطلب أكثر من وسيلة تحقق للدخول إلى الأنظمة، مما يقلل من فرص الاختراق الناجمة عن سرقة كلمات المرور. كما تتضمن حوكمة المعلومات وضع خطط استجابة للهجمات السيبرانية، بحيث يكون هناك إجراءات طوارئ واضحة لاستعادة البيانات وحماية الأنظمة عند التعرض للاختراق. في المكتبات الأكاديمية تساعد هذه التدابير على حماية بيانات المستخدمين، وسجلات الاستعارة، والموارد البحثية، مما يضمن استمرارية الخدمات الرقمية بأمان، ويعزز الثقة في البنية التحتية التقنية للمكتبة. ومن خلال هذه الجهود، يمكن للمؤسسات الأكاديمية والمكتبات الجامعية تقليل المخاطر الأمنية وضمان بيئة معلوماتية محمية وموثوقة.[1]

3.4.2 الإمتثال للقوانين والتشريعات في حوكمة المعلومات.

تهدف حوكمة المعلومات إلى الامتثال للقوانين والتشريعات الخاصة بحماية البيانات جزءًا أساسيًا من حوكمة المعلومات، حيث تفرض القوانين الدولية والمحلية معايير صارمة لضمان الاستخدام الآمن والمسؤول للبيانات. ويُعد الالتزام بهذه المعايير ضروريًا لحماية حقوق الأفراد والمؤسسات وتقليل المخاطر القانونية التي قد تنجم عن إساءة استخدام البيانات أو تسريبها[2].

من أبرز هذه القوانين اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، والتي تنظم كيفية جمع البيانات الشخصية واستخدامها، وتفرض عقوبات صارمة على المخالفين. كذلك، توفر شهادة ISO 27001 إطارًا شاملًا لإدارة أمن المعلومات (ISMS)، مما يساعد المؤسسات على وضع سياسات واضحة لحماية البيانات. بالإضافة إلى ذلك، تلعب قوانين حماية حقوق الملكية الفكرية دورًا محوريًا في المكتبات الجامعية والمراكز البحثية، حيث تحافظ على حقوق النشر والاستخدام القانوني للمحتوى الرقمي والمصادر الأكاديمية.[3]

وبالتالي الامتثال لهذه القوانين يعزز حماية حقوق المستخدمين، ويقلل من المخاطر القانونية والمالية، ويزيد من ثقة المستفيدين بالمؤسسات الأكاديمية. كما أنه يسهم في بناء بيئة معلوماتية آمنة ومستدامة، تدعم الشفافية والأمان في التعامل مع البيانات، مما يضمن استمرارية الأنشطة الأكاديمية والبحثية وفق معايير الحوكمة الرشيدة.

4.4.2 دعم إتخاذ القرار وتحليل البيانات.

أصبحت تحليل البيانات واتخاذ القرارات المستندة إلى المعلومات الدقيقة من الركائز الأساسية لنجاح المؤسسات الأكاديمية والإدارية. تساعد حوكمة المعلومات في ضمان توفر بيانات موثوقة ودقيقة، مما يمكن الجامعات

---

[1] . سلطان، إبراهيم. **المرجع السابق**. ص 12 – 13

[2] . بن محمد، هدى؛ كورتل، نجاة. **المرجع السابق**. ص 182

[3] . بن محمد، هدى؛ كورتل، نجاة. **المرجع السابق**. ص 182

والمكتبات من تحليل الاتجاهات، والتخطيط الاستراتيجي، واتخاذ قرارات قائمة على المعرفة بدلاً من التقديرات العشوائية. ويتم تحقيق ذلك من خلال تنظيم البيانات، وتوحيد معايير تخزينها، وتسهيل الوصول إليها، مما يسمح للقيادات الأكاديمية بتحليل الأداء في مجالات مثل إدارة الموارد المالية، وتطوير الخدمات التعليمية، وتحسين تجربة الطلاب والباحثين. كما أن البيانات المنظمة بشكل جيد تساعد في التنبؤ بالمستقبل وتحديد الاتجاهات الناشئة، مما يدعم الابتكار في المناهج الدراسية وأساليب التدريس، ويوفر رؤية واضحة حول احتياجات الطلاب والمجتمع الأكاديمي. في النهاية، تسهم هذه الجهود في تعزيز الكفاءة التشغيلية واتخاذ قرارات أكثر دقة واستدامة، مما يعزز من قدرة المؤسسات على مواجهة التحديات المستقبلية بفعالية.[1]

5.4.2 تعزيز إستمرارية الأعمال وتقليل المخاطر التشغيلية.

في ظل التحديات الرقمية المتزايدة، أصبحت حوكمة المعلومات عنصرًا أساسيًا لضمان استمرارية الأعمال وتقليل المخاطر التشغيلية في المؤسسات، لا سيما في البيئات الأكاديمية مثل المكتبات الجامعية. تسهم حوكمة المعلومات في وضع استراتيجيات متكاملة للطوارئ تشمل خطط استعادة البيانات بعد الكوارث والأعطال التقنية أو الهجمات الإلكترونية، مما يضمن استمرار تشغيل الأنظمة الرقمية دون توقف. ويشمل ذلك إنشاء نسخ احتياطية آمنة للبيانات يتم تحديثها دوريًا، بالإضافة إلى تفعيل خطط استجابة سريعة للحوادث السيبرانية لضمان الحد الأدنى من التأثير على الخدمات الأكاديمية والإدارية.[2]

إلى جانب ذلك، تعمل حوكمة المعلومات على إدارة دورة حياة البيانات بفعالية، حيث يتم تصنيف البيانات وفقًا لأهميتها، مما يسمح بالاحتفاظ بالمعلومات الضرورية فقط، وحذف أو أرشفة البيانات غير الضرورية بطريقة آمنة. هذه العملية تقلل من مخاطر فقدان البيانات أو تسربها، خاصة في المؤسسات التي تتعامل مع معلومات حساسة مثل سجلات الطلاب، الأبحاث الأكاديمية، والمصادر الرقمية. كما يساعد ذلك في تحسين كفاءة إدارة البيانات عبر تقليل التكرار غير الضروري للمعلومات، وتخفيف الحمل على أنظمة التخزين، وضمان توافق البيانات مع القوانين والتشريعات الخاصة بحماية المعلومات.[3]

في المكتبات الأكاديمية، تلعب هذه الإجراءات دورًا حيويًا في ضمان استمرارية الخدمات التعليمية والبحثية، حيث تتيح إمكانية الوصول المستمر إلى الفهارس الرقمية، قواعد البيانات العلمية، والموارد الإلكترونية حتى في حال حدوث مشكلات تقنية أو اختراقات أمنية. كما أن وجود خطط طوارئ واضحة يعزز ثقة المستخدمين في قدرة المؤسسة على إدارة البيانات بكفاءة، مما يسهم في تعزيز الابتكار وتحسين تجربة الباحثين والطلاب. بالتالي، فإن تطبيق حوكمة المعلومات بفعالية لا يقتصر فقط على الحماية الأمنية، بل يمتد ليشمل تحسين استدامة

---

1. EL Qasmi, Mohamed Jaouad. Kriouile, Abdelaziz.OP.Cit. P 130- 131
2. EL Qasmi, Mohamed Jaouad. Kriouile, Abdelaziz. **Op.Cit**. P 132
3. غنيمات، رغد. **المرجع السابق**. ص 143

الخدمات، وضمان التشغيل السلس للأنظمة، ودعم استمرارية العمل في بيئات ديناميكية تتطلب جاهزية عالية لمواجهة المخاطر التقنية والأمنية.[1]

6.4.2 تحسين الكفاءة التشغيلية وتقليل التكاليف.

تلعب حوكمة المعلومات دورًا محوريًا في تحسين الكفاءة التشغيلية وتقليل التكاليف داخل المؤسسات الأكاديمية والبحثية، حيث تهدف إلى تنظيم وإدارة البيانات بطريقة فعالة تسهم في تقليل الفوضى، وتجنب التكرار، وتحسين استخدام الموارد المتاحة. عندما تكون المعلومات مرتبة وفق معايير موحدة، ومخزنة بشكل منظم، ومحدثة بشكل دوري، تصبح إدارتها أكثر سهولة وكفاءة، مما يقلل من الحاجة إلى التدخل اليدوي المتكرر ويزيد من سرعة الوصول إلى البيانات المطلوبة. هذا بدوره يختصر الوقت المستغرق في معالجة المعلومات، ويقلل من الأخطاء الناتجة عن تكرار البيانات أو فقدانها، مما يسهم في رفع إنتاجية الموظفين وتقليل التكاليف التشغيلية المرتبطة بإدارة البيانات غير المنظمة.[2]

إلى جانب ذلك، تعتمد المؤسسات الحديثة على إستراتيجيات التخزين الذكية مثل استخدام الحوسبة السحابية والتقنيات الرقمية الحديثة، مما يساعد في تقليل الحاجة إلى البنية التحتية التقليدية مثل الخوادم المادية وأنظمة التخزين المكلفة. توفر الحوسبة السحابية مزايا متعددة، من بينها التخزين المرن، وإمكانية التوسع حسب الحاجة[3].وخفض تكاليف الصيانة والتحديث، حيث لا يتعين على المؤسسات الاستثمار بشكل مكثف في شراء وتحديث الأجهزة بشكل دوري. علاوة على ذلك، تتيح هذه التقنيات الوصول إلى البيانات من أي مكان وفي أي وقت، مما يعزز كفاءة العمل عن بُعد ويقلل من الحاجة إلى مساحات تخزين ضخمة داخل المؤسسات.[4]

في المكتبات الجامعية، تسهم هذه المبادئ في تحسين إدارة الموارد الرقمية، حيث تساعد في تقليل الحاجة إلى الفهارس الورقية، وتسريع عمليات البحث عن الكتب والمصادر العلمية، وضمان حفظ البيانات بطريقة آمنة وموثوقة. كما أن استخدام الذكاء الاصطناعي وأدوات تحليل البيانات يساعد في تحسين عمليات الأرشفة، والتصنيف التلقائي للمصادر، وتقديم توصيات ذكية للمستخدمين، مما يسهم في تحسين تجربة الباحثين والطلاب ويزيد من فعالية استخدام الموارد. بالتالي فإن تطبيق حوكمة المعلومات بفعالية لا يحقق فقط الاستدامة المالية عبر

---

[1] . غنيمات، رغد. **المرجع نفسه**. ص 144

[2] . خلفلاوي، شمس ضيات. **المرجع السابق**. ص 125

[3] . سرير عبد الله، ناذير ؛ رحمونة، بوشتة. **المرجع السابق**. ص 20

[4] . سرير عبد الله، ناذير ؛ رحمونة، بوشتة. **المرجع نفسه**. ص 20

تقليل النفقات التشغيلية، ولكنه أيضًا يعزز الكفاءة التنظيمية، ويرفع من جودة الخدمات المقدمة، ويدعم اتخاذ القرارات المستندة إلى البيانات الدقيقة.[1]

التعاون المؤسسي وتكامل البيانات في حوكمة المعلومات: تهدف حوكمة المعلومات الى تعزيز التعاون المؤسسي وتكامل البيانات، حيث تسهم في تسهيل تبادل المعلومات بين الإدارات المختلفة داخل المؤسسة، وكذلك بين المؤسسات الأكاديمية والبحثية. عندما يتم تنظيم البيانات وفق معايير موحدة، يصبح من السهل الوصول إليها والاستفادة منها عبر مختلف الجهات، مما يعزز كفاءة العمل الجماعي ويسهل تنفيذ المشاريع البحثية المشتركة. على سبيل المثال: في الجامعات والمكتبات الأكاديمية، يساعد تكامل أنظمة إدارة البيانات على ربط قواعد البيانات البحثية، مما يتيح تدفق المعلومات بسلاسة بين الأساتذة، الباحثين، والطلاب، وبالتالي يسرّع عمليات البحث والتحليل العلمي.[2]

علاوة على ذلك، فإن توحيد معايير البيانات يضمن أن المعلومات المخزنة عبر الأنظمة المختلفة متسقة ودقيقة، مما يقلل الأخطاء والتكرار، ويسهم في تعزيز الشفافية والموثوقية في إدارتها. من خلال هذه الحوكمة الفعالة، تصبح المؤسسات الأكاديمية أكثر تنظيمًا وكفاءة، حيث يمكن اتخاذ قرارات مستنيرة بناءً على بيانات موحدة ودقيقة. كما يؤدي تحسين إمكانية الوصول إلى المعلومات إلى تحفيز الابتكار العلمي، من خلال تمكين الباحثين من استكشاف مصادر جديدة والتعاون في دراسات متعددة التخصصات، مما يعزز التطور المستدام للبحث العلمي والمعرفة في مختلف المجالات.[3]

5.2 مبادئ وأبعاد حوكمة المعلومات:

تضمن مبادئ وأبعاد حوكمة المعلومات الإشراف على إدارة المشاريع وتصنيف المعلومات وسلامتها وأمنها وإمكانية الوصول اليها والتحكم بها ومتابعتها وتدقيقها وتطوير السياسات الخاصة بها وتحسينها بشكل متواصل، وتتمثل مبادئ حوكمة المعلومات في مايلي:

1.5.2مبدأ المساءلة:

---

1. Makhlouf Shabou, Basma.**Ibid**. P 09
2. Makhlouf Shabou, Basma. **OP**.**Cit**. P 12
3. الصباغ، عماد عبد الوهاب. **المرجع السابق**. 39

يقصد بمبدأ بضرورة وجود نظام متكامل من المحاسبة والمسائلة السياسية والإدارية للمسؤولين في وظائفهم العامة، لحماية الصالح العام من التعسف والاستغلال السياسي[1].

تسمح بكشف التلاعب أو الفساد بمعدل أسرع من المعتاد. وتنبه المسئولين بالحذر والحيطة في أعمالهم طالما أن المسائلة متسعة المصادر. كما أن أهمية المساءلة تكمن في قدرتها على حماية المصالح العامة بشكل أكثر فعالية وتأكيد وتطبيق مبادئ الديموقراطية. ومن الوسائل المستعملة لتحقيق المسائلة نذكر مجالس التقييم والرقابة.[2]

يغطي مبدأ المساءلة المسؤولية المخصصة من أجل إدارة السجلات على مستوى الإدارة العليا لضمان الحوكمة الفعالة بمستوى مناسب من الصلاحيات. بحيث يجب أن يشغل كبير المديرين التنفيذيين منصبا مرموقا بما فيه الكافية في الهيكل التنظيمي للمؤسسة، كي يتمتع بالصلاحيات الكافية من أجل تفعيل برنامج إدارة السجلات بشكل ناجح. ويقتضي الدور الرئيسي الذي يؤديه كبير المديرين التنفيذيين وضع سياسات وإجراءات وتوجيهات الإدارة السجلات وتطبيقها مع تقديم الارشادات والنصائح حول المسائل المتعلقة بحفظ السجلات وكفية حمايتها. ويحق لكبير المديرين التنفيذيين تفويض المسؤولية المباشرة لإدارة أو تشغيل المنشآت أو خدمات.[3]

يجب أن يكون لدى كبير المديرين التنفيذيين فهم للأعمال والبيئة التشريعية التي تعمل ضمنها المؤسسة وتقوم بتنفيذ مهامها وأنشطتها وأعماله والعلاقات المطلوبة مع أصحاب المصلحة الخارجين الاساسين لفهم الطريقة التي تساهم بها إدارة السجلات في تحقيق رسالة الشركات وأهدافها وبلوغ غايتها.[4]

كما يجب أيضا تحديد الإطار التنظيمي والقانوني للإدارة السجلات وفهمه بوضوح. بحيث أن يكون لدى كبير المديرين التنفيذيين اطلاع جيد على معلومات الشركة وهيكلها التقني ويجب أن تشارك بشكل فعال في اتخاذ القرارات الاستراتيجية للحصول على نظم تقنية المعلومات وتشغيلها.[5]

من المهم للمديرين التنفيذيين في الإدارة العليا حيازة المسائل المتعلقة بإدارة السجلات في المؤسسة وتحديد الإجراءات التصحيحية اللازمة للتقليل من وقوع المشاكل أو ضمان حلها أو التصدي لتحديات حفظ

---

[1]. محاجبي. عيسى. **مبادئ تطبيق اخلاقيات الحوكمة وأثرها على تحسين الأداء في المكتبات الأكاديمية في الجزائر**. رسالة الماجستير: قسم علم المكتبات. جامعة الجزائر 02، 2020. ص 60

[2]. محاجبي. عيسى. **المرجع السابق**. ص 60

[3]. بن خضير، أحمد بن عبد الله. **المرجع السابق**. ص 38

[4]. عقوق، شراف؛ دوفي، قرمية. **حوكمة الشركات ودورها في استقرار الأعمال**. مجلة الأصيل للبحوث الاقتصادية والإدارية. المجلد، 04. العدد، 02، 2020. ص 20

[5]. انتر، فارماكول. **حوكمة المعلومات: إدارة المخاطر، والامتثال**. المجلد، 06. العدد، 03، 2018. ص 192_193

السجلات. كما يجب على المشرف التنفيذي على إدارة المشاريع اغتنام الفرص لرفع الوعي بأهمية إدارة السجلات وإبلاغ الموظفين والإدارة بفوائد الإدارة الجيدة للسجلات.[1]

كذلك نجد مفهوم المساءلة يهدف إلى وجود طرق مؤسسية تمكن من مساءلة الشخص المسؤول ومراقبة أعماله وتصرفاته في إدارة الشئون العامة، مع إمكانية القيام بإقالته إذا تجاوز السلطة أو أخل بثقة الناس وهذه المساءلة نكون مضمونة بوجود القانون ومتحققة بوجود قضاء عادل مستقل ومحايد ومنصف. ولكنها تستهدف قدرة تمكين ذوي العلاقة من متابعة ومساءلة الموظفين والمسؤولين عن طريق القنوات والأدوات المناسبة، دون أن يؤدي ذلك الى تعديل العمل. فمبدأ المساءلة مرتبط بمساءلة كل من يقوم بارتكاب الأخطاء من خلال تفعيل القوانين والأنظمة دون أن تقتصر الى جانب العقاب وانما يجب أن ترتكز الى جانب الثواب أيضا، كحافز للمسؤولين على أداء مهامهم بإخلاص واتقان.[2]

يأخذ كبير المديرين التنفيذيين على عاتقه مسؤولة التأكد من استخدام العمليات والإجراءات وأنظمة الحوكمة والوثائق ذات الصلة. ويجب ان تحدد السياسات الأدوار والمسؤوليات على جميع المستويات في المؤسسة[3].

ويجب استخدام عملية الفحص والتدقيق كي تغطي الجوانب إدارة السجلات كافةداخل المؤسسة بها في ذلك التأكد من تعيين مستويات كافية من المساءلة وتحديد نقاط الضعف والقصور في المساءلة ومعالجتها. ويجب أن تتضمن عمليات الفحص والتدقيق الامتثال لسياسات الشركة واجراءاتها لجميع السجلات بصرف النظر عن صيغتها او الوسيلة التي تم حفظها عليها. تضم متطلبات الفحص والتدقيق في المساءلة بالنسبة للسجلات الالكترونية استخدام تقنية مناسبة لفحص بنية المعلومات وأنظمتها وتدقيقها. ويجب تحديث أنظمة المساءلة والمحافظة عليها نتيجة للتغيرات التي تطرأ على البنية التحتية للتقنية.[4]

2.5.2 مبدأ الشفافية :

---

[1] . جيرار، بيرو. **إدارة السجلات والمحفوظات في الأمم المتحدة**. جنيف: الأمم المتحدة، 2013

[2] .الشباطات، محمد علي. **مفهوم حوكمة الجامعات وأثره في تعزيز معايير الشفافية والمساءلة والمشاركة**. مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي. المجلد، 38. العدد، 02، 2018. 154

[3]. بن خضير، أحمد بن عبد الله. **المرجع السابق**. ص 39

[4]. بن خضير، أحمد بن عبد الله. **المرجع نفسه**. ص 39

يشير مفهوم الشفافية الى سهولة الوصول الى المعلومات والافصاح عنها، ويعني المفهوم من اتجاه اخر استخدام الطريقة العلنية في مناقشة الموضوعات وحرية تداول المعلومات. وأن تتوافر المعلومات الكافية لتفهمها ومراقبتها ومتابعتها.[1]

وتعد الشفافية من المفاهيم الحديثة والمتطورة في حوكمة المعلومات والتي يجب على الإدارة الواعية الأخذ بها لما لها من أهمية على مرفق الجامعة والأطراف المعنية بها. وتعني الشفافية الانفتاح والتخلي عن الغموض والسرية والتضليل، وجعل كل شيء قابلا للتحقق والرؤية السليمة. وبهذا المعنى فالشفافية ما هي الا وضوح لما يجري ويدور داخل المؤسسة، مع سهولة تدفق المعلومات الدقيقة والموضوعية وسهولة استخدامها وتطبيقها فعلا من قبل الموظفين. هذا الوضوح يعني الموظفين في المؤسسات يستطيعون وبكل سهولة الإفصاح لقيادة المؤسسة عما يدور بخلدهم وعن مشكلاتهم واحتياجاتهم، مما يولد حوارا منتجا ما بين قيادات المؤسسة والموظفين. وتشكل اللقاءات المفتوحة تحديا لتفكير العاملين وتحفزهم على المشاركة وتسهم في تغطية قيم الحوار والتواصل البناء ما بين قيادات المؤسسة والعاملين فيها.[2]

تعتبر السياسات بمكانة الارشادات والتوجيهات الخاصة بعمل المؤسسة وادارتها، وتقدم دليلا أساسيا للعمل الذي يرسم الحدود التي يجب أن يتم تنفيذ أنشطة الأعمال ضمنها. وتحدد ذلك السياسات مسار العمل الذي يجب أن تتبعه المؤسسة ووحدات الأعمال والأقسام والموظفون[3].

وبالتالي مبدأ الشفافية يعتبر عامل أساسي لحوكمة المعلومات والامتثال للقوانين. لذلك يجب أن تكون الوثائق متناسقة حديثة وكاملة. ويجب أن تضمن عملية المراجعة والموافقة أن طرح البرامج أو التغييرات الجديدة قابل للتنفيذ والمج في عمليات الأعمال.[4]

وكون أن الشفافية تتضمن الممارسات الخاصة بحفظ السجلات توثيق العمليات والتشجيع على الفهم الأدوار والمسئوليات لأصحاب المصلحة كافة. يجب أن تكون السياسات المؤسسة ذات طابع رسمي ويتم دمجها في

---

[1]. صمود سيد أحمد. لحمر خالد. **دور حوكمة الشركات في تطبيق مبدأ الإفصاح والشفافيةاتجاه المساهمين**. مجلة الدراسات الحقوقية. المجلد، 07. العدد، 02، 2020. ص 586

[2]. يعقوب عادل، ناصر الدين. **إطار مقترح لحوكمة الجامعات ومؤشرات تطبيقها في ضوء متطلبات الجودة الشاملة**. مجلة تطوير الأداء الجامعي. المجلد، 01. العدد، 02، 2012. ص 94_ 95

[3]. السبيعي، فلاح بن فرج. **أثر تطبيق الشفافية الإدارية في الحد من الفساد الإداري في الشركات المالية السعودية**. المجلد، 37. العدد، 01، 2017. ص 186

[4]. السبيعي، فلاح بن فرج. **المرجع نفسه**. ص 186

عمليات الأعمال لتكون فعاليتها أكبر. ولا بد من ابلاغ الموظفين بقواعد الاعمال ومتطلبات حفظ السجلات وتطبيقها

على مستويات المؤسسة كافة[1].

بالإضافة الى ذلك يجب أن يكون لدى الموظفين الاطلاع بالسياسات والإجراءات الخاصة بإدارة السجلات، ويجب أن يحصلوا على التوجيهات التثقيفية والتدريبات اللازمة لضمان فهم مسؤولياتهم وأدوارهم ومتطلبات إدارة السجلات. كما يجب تطوير أنظمة حفظ السجلات وعمليات الأعمال لتحديد دورة حياة السجلات بوضوح.[2]

فضلا على هذا الى السياسات والإجراءات والارشادات والتوجيهات التشغيلية، يجب أن تتضمن الجداول وخرائط سير المعلومات ووثائق وكتيبات المستخدمين توجيهات واضحة حول كيفية انشاء السجلات وحفظها وتخزينها والتخلص منها. ويجب أن تتمتع هذه الوثائق بالجاهزية والاتاحة ومتضمنة في البيانات والتدريبات التي يتم تقديمها للموظفين.[3]

وتكمن أهمية تطبيق مبدأ الشفافية في مايلي:

- تحقيق المصلحة العامة فغياب الشفافية في بعض التشريعات والقوانين وعدم وضوح النصوص بهذه التشريعات والأنظمة في المؤسسات، يعتبر سببا رئيسيا للاجتهادات الشخصية وبشكل لا يخدم المصلحة العامة.
- المساعدة في اتخاذ القرارات الصحيحة، ذلك أن عدم مراجعة الدورية للقوانين والأنظمة بشكل واضح وبشكل يواكب المستجدات العصرية في بيئات الأعمال يترتب عليه اتخاذ قرارات إدارية سريعة وغير سليمة ولا تستند الى المرجعية العلمية الأمر الذي يعرقل عمليات التنمية الإدارية والشاملة لذلك. فلابد من وجود الشفافية داخل المؤسسات.
- تعمل الشفافية على المشاركة في اتخاذ القرارات وتسمح بتوعية المواطنين واطلاعهم على الخيارات المتاحة. وتحقق العدالة في تقييم أداء العاملين والوصول الى ما يعرف بالنظام المفتوح، إضافة الى كونها الية لتحقيق المساءلة.

---

[1] . رمزي، فهد بن عبد الرحمان مسفر. **الإدارة بالشفافية لدى مديري مكاتب التربية والتعليم بمنطقة مكة المكرمةمن وجهة نظر المديرين والمشرفين**. مذكرة ماجستير. كلية التربية: قسم الإدارة التربوية والتخطيط. جامعة أم القرى. السعودية، 2013.ص 32

[2] . رمزي، فهد بن عبد الرحمان مسفر. **المرجع السابق**.ص 32

[3]. رمزي، فهد بن عبد الرحمان مسفر. **المرجع نفسه**. ص 34

- لقد أحدث حفظ السجلات ثورة كبيرة في المؤسسات وهذا راجع لتطبيق مبدأ الشفافية مما ساهمت في تخزين جميع البيانات والمعلومات المتعلقة بالمؤسسات وهذا بغرض تسهيل على العاملين الوصول اليها[1].

3.5.2 مبدأ السلامة :

مبدأ السلامة في حوكمة المعلومات هو أحد المبادئ الأساسية التي تحكم كيفية إدارة وتأمين البيانات الرقمية والسجلات داخل المؤسسات. ويشير هذا المبدأ الى مجموعة الإجراءات والسياسات التي تهدف الى حماية المعلومات من التهديدات المختلفة مثل الاختراقات، والفيروسات، والوصول غير المصرح به. وتكمن أهمية هذا المبدأ في حماية الأصول الرقمية وحفظ السجلات لأي مؤسسة سواء كانت بيانات عملاء، أو المعلومات المالية، أو الملكية الفكرية. كذلك الامتثال للقوانين واللوائح لأنها تلزم المؤسسات بحماية بيانات العملاء والمعلومات الحساسة. فضلا على ذلك منع أي اختراق أمني يمكن أن يؤدي الى فقدان الثقة في المؤسسة وتضرر بسمعتها، بالإضافة الى أن مبدأ السلامة يساهم وبشكل كبير في ضمان استمرارية الأعمال وإدارة المخاطر المحتمل وقوعها.[2]

يتم تطبيق مبدأ السلامة من خلال مجموعة من الإجراءات التقنية والإدارية والتي تتمثل فيما يلي:

- يجب تقويم أنظمة انشاء السجلات لتحديد إمكانيات حفظ السجلات.
- يجب اعداد وتجهيز عملية رسمية لاكتساب أنظمة جديدة وتطويرها بما في ذلك متطلبات جمع البيانات الوصفية اللازمة لإدارة دورة حياة السجلات في الأنظمة.
- يجب ان يحتوي السجل على جميع العناصر الضرورية للسجل الرسمي منها البنية والمحتوى وأيضا السياق.
- يجب استخدام برامج مكافحة الفيروسات وجدران الحماية، ونظم الكشف عن الاختراقات، مع تدريب العاملين على أفضل الممارسات الأمنية[3].

ويتم تأكيد سلامة السجلات وموثوقيتها وصدقها من خلال ضمان انشاء سجل من قبل خبير او سلطة مختصة وفقا للعمليات المعروفة والمعمول بها. وبالتالي فان المحافظة على سلامة السجلات تعني أنها كاملة ومحمية من

---

[1]. السبيعي، فلاح بن فرج. **المرجع السابق**. ص188-189

[2]. العسالي، جمال. **تطبيق حوكمة الشركات في المؤسسات الصغيرة والمتوسطة كآلية لتحسين الأداء الاقتصادي في الجزائر2000-2014**. أطروحة دكتوراه. كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير: نقود مالية وبنوك. جامعة الجزائر 03. الجزائر، 2019. ص 30

[3]. العسالي، جمال. **المرجع السابق**.ص44-45

التحريف والتغيير. ويتم تأكيد مصداقية السجلات من الأدلة الداخلية والخارجية بما في ذلك خصائص السجلات وبنيتها ومحتواها وسياقها، للتحقق من مدى مصداقيتها وعدم تعرضها للتحريف أو الاتلاف.[1]

4.5.2 مبدأ الحماية:

يجب أن تضمن المؤسسات حماية السجلات لضمان عدم تغييرها أو تحريفها من خلال تعرضها للتلف أو فقدانها. هذا يتضمن التغييرات التقنية أو تعطل أقراص التخزين الرقمية وحماية السجلات من التلف. حيث أوجد المشرع الجزائري من خلال الأمر 21-09 مجموعة من القواعد ينبغي على السلطات المعنية المتمثلة في الدولة ومؤسساتها وهيئاتها مثلما وضحتها المادة 02 من هذا الأمر وعلى الغير أيضا مراعاتها، حيث تستهدف هذه القواعد حماية المعلومات والوثائق الإدارية وذلك لتأمينها والحفاظ على سريتها بعدم افشائها لاسيما الوثائق المصنفة منها والمبينة بمقتضى المادة 06 من هذا الأمر والتي عددتها الى وثائق "سري جدا"، "سري"، "وواجب الكتمان"، "وتوزيع محدود"، وقد أشارت المواد الى 7-13 الى مختلف تلك القواعد أو الالتزامات التي من خلالها تتجسد هذه الحماية الوقائية، كذلك نصت المادة 07 من الأمر 09-12 على الالتزام بتأمين الوثائق والمعلومات والحماية الأرشيفية، حيث جاء فيها:" تلزم السلطات المعنية بتأمين وثائقها ومعلوماتها وحمايتها،

وتتخذ التدابير اللازمة لتصنيف وتنظيم تداولها وحفظها وفقا للأحكام المنصوص عليها في التشريع والتنظيم المعمول بها ولاسيما ما يتعلق منها بالأرشيف الوطني[2].

من خلال نص هذه المادة نجد المشرع ألقى على عاتق الإدارة الزاما بتأمين المعلومات والوثائق لاسيما المصنفة منها واتخاذ مجموعة من التدابير اللازمة الرامية للحماية السجلات والوثائق، ان هذا الالزام يقتضي اختصارا اتباع قواعد معنية تدعى بعملية إدارة الوثائق والتي تعرف بأنها تنظيم وترتيب للوثائق بوضع الخطط والأساليب والطرق الفنية والعلمية في عملية انتاجها وكيفيات استرجاعها.[3] مع وضع الضوابط وتطبيقها ومتابعتها ومراجعتها للوصول الى المعلومات وحمايتها لضمان استمرارية الأعمال والحد من التأثير المخاطر في الأعمال. تحتوي القيود المفروضة على الوصول الى المعلومات والكشف عنها على طرق لحماية خصوصية الأفراد والمعلومات التي يملكونها. كما يجب دمج متطلبات الوصول في نظم الأعمال وعملياتها من أجل انشاء السجلات واستخدامها وتخزينها. وذلك باستخدام أنشطة حفظ المعلومات الرقمية لمدة طويلة LTDB التي هي عبارة عن مجموعة أنشطة ضرورية

---

[1] . العسالي، جمال. **المرجع نفسه**. ص45

[2]. الأمر 21- 09 المؤرخ في 27 شوال 1441 الموافق ل 08 يونيو 2021.**يتعلق بحماية المعلومات والوثائق الإدارية**. عدد45 الصادرة في 09 يونيو 2021

[3] . بن فردية، محمد. **اليات حماية المعلومات والوثائق الإدارية دراسة من خلال أحكام الأمر 21-09**. المجلة الدولية للبحوث القانونية والسياسة. المجلد،05. العدد، 03، 2021. ص120 _ 121

لضمان الوصول باستمرار الى المواد الرقمية طوال وقت الحاجة اليها. ان السجلات الالكترونية التي يجب حفظها لمدة طويلة قد تستلزم تحويلها صيغة مناسبة لضمان الوصول اليها وإمكانية قراءتها على المدى الطويل.[1]

5.5.2 مبدأ الإمتثال للقوانين :

تضمن برامج إدارة السجلات العمل على تطوير المكونات الأساسية وتدريب عليها مثل مراقبة الامتثال للقوانين لضمان استمرارية البرنامج. يمكن متابعة الامتثال للقوانين ومراقبته من قبل مدقق داخلي او مؤسسة خارجية أو إدارة السجلات RM بصورة منتظمة وهذا يعني ان المؤسسات يجب أن تتبع قواعد محددة حول كيفية حفظ السجلات ومدى الوقت الذي يجب الاحتفاظ بها فيه. عدم الامتثال لهذه القوانين يمكن أن يؤدي الى عواقب قانونية ومالية. وبالتالي يهدف هذا المبدأ الالتزام بتكوين الموظفين في مجال استعمال الوثائق المصنفة وهذا ما أكدت عليه المادة 07 من القانون 88-09، حيث يختص هذا الالتزام في ضرورة تكوين الموظفين في اتباع أحدث الطرق وكذا ادخال استعمال الوسائل التكنولوجية في عملية الحفظ والتصنيف والتأمين والسجلات والوثائق[2].

وفي هذا الإطار وبغية الوصول لتلك الأهداف وجب على السلطات المعنية المبنية في هذا القانون احداث دورات تدريبية للموظفين التابعين لها والسهر على ضمان الوسائل اللازمة لهم في هذا المجال، وينبغي التنويه عموما أنه مع تطور الوثائق تطورت أساليب الحفظ والحماية لها.[3]

تنطوي متابعة الامتثال للقوانين على حفص العديد من جوانب إدارة السجلات وتدقيقها بها في ذلك ضمان انشاء السجلات وجمعها بشكل صحيح، وتطبيق أدونات المستخدمين وإجراءات الأمن، وعمليات سير العمل من خلال أخذ العينات لضمان الامتثال للسياسات والإجراءات وضمان حفظ السجلات بعد الوصول على تصريح بإتلافها وتوثيق السجلات التي تم اتلافها أو نقلها لتقرير سواء أكان اتلاف أو نقل السجلات مصرحا بها وفق توجيهات التخلص من السجلات. هذا يشير الى ان إدارة السجلات تتطلب تقييما مستمرا ويجب على

---

[1]. أجعود، سعاد. **تجريم التعدي على سرية المعلومات والوثائق الادارية دراسة تحليلية على ضوء الأمر 21-09 المتعلق بحماية المعلومات والوثائق الإدارية**. مجلة الحقوق والعلوم الإنسانية. المجلد، 15. العدد، 02، 2022. ص 632

[2]. شرقي، فتيحة؛ قموح، فتيحة. **حفظ الأرشيف في الجزائر بين الحمية القانونية والإجراءات الفنية**. مجلة الاتحاد العربي للمكتبات والمعلومات. المجلد، 02. العدد، 09، 2009. ص 09

[3]. شرقي، فتيحة. قموح فتيحة. **المرجع نفسه**. ص 09

المؤسسات أن تقوم بفحص دوري لنظام إدارة السجلات لديها للتأكد من أنه يعمل بكفاءة وفعالية، هذا التقييم أن يتم داخليا من قبل موظفي المؤسسة، أو خارجيا من قبل جهة خارجية متخصصة.[1]

6.5.2 مبدأ توافر السجلات :

يجب أن تقوم المؤسسات بتقويم مدى فعالية وكفاءة طرق تخزين السجلات والمعلومات واستعادتهم عن طريق استخدام المعدات والأجهزة والشبكات والبرامج الموجودة. كذلك يجب أن يحدد التقويم المتطلبات الحالية والمستقبلية ويوصي بالأنظمة الجديدة حسب الاقتضاء. وأيضا دراسة عوامل محددة قبل ترقية أو تنفيذ أنظمة جديدة. تضم هذه العوامل فائدة وتكلفة وفعالية التكوينات الجديدة. من التحديات التي تواجه المؤسسات ضمان الوصول الى المعلومات في الوقت المناسب وبشكل موثوق واستخدامها، وأن السجلات تكون متاحة وقابلة للاستخدام طوال مدة حفظها ويساهم في وجود هذا التحدي التغييرات السريعة والتحسينات التي تطرأ على الأجهزة والبرامج. بالإضافة الى توفير المعلومات الدقيقة والكاملة في الوقت المناسب يساعد صناع القرار على اتخاذ قرارا مدروسة وفعالة فضلا على ذلك الحفاظ على سمعة المؤسسة من خلال ضمان توافر المعلومات يمكن أن يحمي المؤسسة من المخاطر القانونية والمالية، ويحافظ على سمعتها.[2]

7.5.2مبدأ حفظ السجلات :

مرحلة حفظ السجلات: هو المهمة المعنية للاستمرار في استخدامها. ويعمل جدول حفظ السجلات على تحديد الإجراءات اللازمة لتحقيق متطلبات حفظ السجلات والتخلص منها، ويمنح الموظفين صلاحيات ويوفر لهم أنظمة لحفظ السجلات واتلافها ونقلها. ويعمل جدول حفظ السجلات على توثيق متطلبات حفظ السجلات وإجراءات محددا بذلك، وكيفية ترتيب السجلات وحفظها، وما يجب حدوثه للسجلات، ووقت حدوث ذلك، وتحديد هوية الشخص المسؤول عن القيام بهذه العلمية وهوية الشخص الذي يجب الاتصال به للإجابة عن الأسئلة والحصول على التوجيهات. ويجب أن تحدد المؤسسات نطاق متطلبات حفظ السجلات من أجل توثيق أنشطة الأعمال بناء على الأنشطة المنظمة والسلطات القانونية التي تفرض الرقابة على السجلات.[3]

---

[1]. عباسي، محمد الحبيب. **الحماية الجزائية للمعلومات والوثائق الإدارية من خلال الأمر 21-09**. مجلة القانون والعلوم السياسية. المجلد، 09. العدد، 01، 2023. ص 420

[2]. العسالي، جمال. **المرجع السابق**. ص 84

[3]. الورفلي، طارق. **برنامج تدريس إدارة الوثائق والمحفوظات بجامعة الشرقية**. المجلد، 12. العدد، 02، 2020. ص 23

ويشمل هذا أنشطة الأعمال التي تنظمها الحكومة لكل وقع أو نطاق لسلطة قانونية، تمارس ضمنه الشركة أعمالها. كما يشمل الاعتبارات الأخرى لتحديد متطلبات حفظ السجلات واعتبارات تشغيلية وقانونية ومالية وتاريخية وهي كمايلي:

1. مرحلة مدة حفظ السجلات: هي المدة الزمنية التي يجب خلالها حفظ السجلات واتخاذ الإجراءات اللازمة لإتلافها أو الاحتفاظ بها. يجب أن تستند أوقات حفظ السجلات بمختلف أنواعها الى المتطلبات التشريعية والتنظيمية بالإضافة الى المتطلبات الإدارية أو التشغيلية. ومن المهم توثيق الأبحاث والدراسات القانونية التي يتم اجراءها واستخدامها للتأكد سواء أكانت القوانين واللوائح نسبيا تنطبق على ممارسات حفظ السجلات وتقدم الأدلة والبراهين للمسؤولين التنظيميين أو المحاكم على أنه تم اجراء دراسة نافية للجهالة بنية حسنة بهدف الامتثال للمتطلبات المعمول بها.[1]

2. مرحلة تقويم السجلات: هو عملية يتم خلالها تقدير وتقويم قيمة المخاطر التي تنطوي عليها السجلات لتحديد متطلبات حفظ تلك السجلات والتخلص منها. ويجب توضيح الأبحاث والدراسات القانونية في تقارير التقويم. ويمكن القيام بعملية التقويم هذه كجزء من عملية وضح جداول حفظ السجلات وكذلك اجراء مراجعة منتظمة لضمان تحديث المستندات والمتطلبات.[2]

3. مرحلة التخلص من السجلات: وهي المرحلة الأخيرة في دورة حياة السجلات عندما تتحقق متطلبات حفظ السجلات ولا تكون هناك حاجة أو ترجى من السجلات لغايات الأعمال، ويجوز التخلص من السجلات واتلافها. ولكن يجب نقل السجلات التي يلزم حفظها لمدة طويلة أو دائما الى الأرشيف لحفظها. كما يجب تحديد وقت نقل السجلات الورقية أو الاليكترونية من خلال عملية جداول حفظ السجلات. في اغلب الأحيان يلزم اتباع طرق إضافية مثل: نقل السجلات، أو تحويلها لحفظ السجلات الالكترونية. كذلك يجب التخلص من السجلات بطريقة منظمة وامنة ووفق للتوجيهات المرخصة من أجل ذلك. ويجب توثيق عملية التخلص من السجلات واتلافها بشكل واضح لتقديم الأدلة والبراهين التي تثبت اتلافها وفق لبرنامج يتم الاتفاق عليه. ويجب التخلص من السجلات بواسطة طرق تتناسب مع سرية المعلومات التي تحتويها السجلات ووفق للتوجيهات المرخصة من أجل التخلص من السجلات في جدول حفظ السجلات. كذلك يجب الاحتفاظ بمستندات المسار الذي اتبعه المدقق لتوثيق عملية اتلاف السجلات، كما يجب الحصول على شهادات الاتلاف عندما يتلف السجلات أطراف خارجية. وفي حالة لم تكن جداول التخلص من

---

[1] . لطرش، حكيم. قوميد، فتيحة. **إدارة الوثائق الجارية والوسيطة: الأدوات والأساليب جامعة حسيبة بن بوعلي _ الشلف أنموذجا**. مجلة ببليوفيليا للدراسات المكتبات والمعلومات. العدد، 04، 2019. ص 151

[2]. قاشي، خالد. **نظام المعلومات التسويقية بالمؤسسة الاقتصادية الجزائرية**. مجلة الأبحاث الاقتصادية. العدد، 05، 2021. ص 72

السجلات جاهزة يجب الوصول على تصريح خطي قبل اتلاف السجلات. كما يجب أن تحدد الإجراءات الشخص الذي يشرف على عملية التخلص من السجلات.[1]

ويتم التخلص من السجلات بطرق عديدة وهي كالآتي:

- رمي السجلات: هذه الطريقة القياسية لإتلاف السجلات الغير السرية. إذا أمكن ذلك يجب فرم السجلات كافة في فرامة الورق قبل إعادة تدويرها وتجدر الإشارة أنه يمكن فرم السجلات المؤقتة في فرامة الورق.
- فرم السجلات فرامة الورق: يجب اتلاف السجلات السرية والحساسية ضمن ظروف أمنية وصارمة يمكن اتلاف هذه النوعية من السجلات على الصعيد الداخلي أو عن طريق فرمها بطريقة أمنية[2].
- الأرشفة: تستخدم هذه الطريقة مع السجلات التي يلزم حفظها لمدة طويلة ويجب حفظ السجلات التي لها قيمة وأهمية قانونية أو مالية أو إدارية أو تاريخية.
- التصوير: يجب تحويل السجلات الورقية الى سجلات بصيغة رقمية (صور رقمية). وبعد ذلك يجب اتلاف المستندات الورقية الأصلية.
- حذف البيانات: تستخدم هذه الطريقة الخاصة من أجل مجموعات البيانات والمستندات والسجلات التي يجب حذفها من خلال ازالتها وفق معايير محددة وفي أغلب الأحيان تنطبق هذه الطريقة على سجلات الهيكلة الموجودة في قواعد البيانات والاستمارات.[3]

خلاصة الفصل:

[1] . لطرش، حكيم. قوميد، فتيحة. **المرجع نفسه**. ص 184 _ 150

[2]. Laura Dubois, Vivian Tero. **Practical information Governance**: **balancing cost**, **Risk and productivity**, IDC White Paper, 2010: P 05

[3] . Laura Dubois, Vivian Tero.**OP**.**Cit**. P 06

مما سبق نخلص، أن حوكمة المعلومات تشكل إطار تنظيمي متكامل يهدف إلى إدارة المعلومات داخل المؤسسة بطرق وإستراتجيات وقوانين محددة ومضبوطة، تشمل الإطار جميع الأطراف والمساهمين داخل المؤسسة وخارجها بما يرفع قيمتها ويحقق الإمتثال والشفافية في العمل ويدعم السرية وخصوصية المعلومات.

وتتزايد أهمية حوكمة المعلومات في ظل التنامي المتسارع للبيانات والتحول الرقمي ومرجعية المؤسسة في تحقيق أهدافها وتحسين آدائها، مما يجعل المعلومات عنصر أساسي في المؤسسة سواء كانت ربحية أو غير ربحية ولا تقل أهمية عن الموارد البشرية والمادية، ونظرا لمكانة المعلومات ودورها الفعال في المؤسسة تواجه هذه الأخيرة العديد من المخاطر والتهديدات فلضمان أمنها وسلامتها في ظل التحول الرقمي نحو الفضاء المفتوح وكما يطلق عليه أيضا الفضاء

الفصل الثالث:

الأمن السيبراني في المكتبات الجامعية: المخاطر، الإستراتيجية وتقنيات الحماية

الفصل الثالث: الأمن السيبراني في المكتبات الجامعية: المخاطر، الإستراتيجية وتقنيات الحماية

تمهيد

يناقش الفصل أحد أبرز المواضيع التقنية التي لازالت تحضى بدراسة وتحليل وجدل فني وتقني وقانوني، خصوصا أن الأمن السيبراني يتشابك مع حقول معرفية عديدة، وفي هذا الإطار سيتم تسليط الضوء على الأمن السيبراني في بيئة المكتبات نظر لخصوصيتها وأدوارها في إدارة وتسيير مواردها، حيث تعتبر المكتبة الجامعية أحد الهياكل الرئيسية ومصدر المعلومات في الجامعة، وعليه فإن ضمان أمن وحماية مواردها الرقمية ونظمها من المخاطر والتهديدات ضروري لإستمرارية المؤسسة. حيث سيتم التطرق إل الأهداف المحورية لأمن المعلومات في المكتبات الجامعية، وتأثيره على الخدمات المكتبية الرقمية. كما تم الوقوف عل أنواع المخاطر والتهديدات المحتملة في بيئة المكتبات وإستراتيجية إدارتها مع التذكير بالتجربة السعودية الرائدة في المجال العربي، وأيضا تقنيات الحماية والتحديات التي تواجه المكتبات الجامعية.

1.3 الأمن السيبراني في المكتبات الجامعية نظرة عامة:

1.1.3 تعريف الأمن السيبراني

أ.لغة:

الأمن السيبيراني لغويا: مكون من لفظتين: الأمن، السيبراني.

الأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أمن، أمنا، وأمانا، وإطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر أي سلم منه.[1]

السيبيراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة "cyber"لفظة يونانية الأصل مشتقة من كلمة kybernetes بمعنى الشخص الذي يدير ربان السفينة، حيث تستخدم مجازاً للمتحكم."governor"وأشار بعض المؤرخين الي أن أصلها يرجع إلى عالم الرياضيات الأمريكي Wiener Norbert وذلك للتعبير عن التحكم الآلي.[2]

---

[1] . حميدي، حياة؛ طايلب، نسيمة. **مدخل مفاهيمي حول الامن السيبيراني**. مدار للدراسات للاتصالات والرقمية. المجلد،02. العدد، 02، 2022. ص 05

[2] . السمحان، منعبد الله بن صالح. **متطلبات تحقيق الأمن السيبيراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**. مجلة كلية التربية. العدد، 111، 2020. ص 08

يعرف معجم OXFORD الإنجليزي على أنها "دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، فيما يعرفها قاموس مصطلحات الأمن المعلوماتي "هجوم الفضاء الإلكتروني يهدف إلى السيطرة على المواقع إلكترونية أو بني محمية إلكترونيا لتعطيلها أو تدميرها أو الإضرار."[1]

أستخدمت في الماضي للدلالة على كيفية تواصل الآلات والكائنات الحية مع بعض وتحكمها. ومن تلك الكلمة نشأت مصطلحات كثيرة أستخدمت في قصص وأفلام الخيال العلمي أو الفضاء السيبيراني والذي يستخدم عادة للإشارة إلى الانترنيت وشبكات الاتصالات وكأنها فضاء وهمي أو إفتراضي. ونظرا لحداثة الاتجاه تولدت الكثير من المفاهيم المرتبطة به والمصطلحات التي تحدد ماهيته بشكل دقيق. وقد أصدرت الهيئة الوطنية للأمن السيبيراني 27 مصطلح: الفضاء السيبيراني، صمود الأن السيبيراني، أمن المعلومات، هجوم سيبراني، دفاع أمني متعدد المستويات...وغيرها.[2]

ب. إصطلاحا:

وردت العديد من التعاريف حول الأمن السيبيراني،كما يعرفبأنه: المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو الغاؤها أو سوء استخدامها أو الفشل في استخدامها أو الوصول اليها أو اظهارها أو مراقبتها أو نسخها أو سرقتها.[3]

يُعرف كذلك بأنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث تتوقف عجلة الإنتاج أو تتحول الأضرار إلى خسائر دائمة". [4]

---

1. قاموس اكسفورد.معجم اكسفورد. بريطانيا: جامعة أكسفورد، 2019.ص 124

2. توفيق محمود محمد، القزاز. **الأمن السيبيراني لمصادر المعلومات**. طبعة،01. القاهرة. مؤسسة طيبة للنشر والتوزيع، 2022. ص 57

3. الطائي، محمدعبد الحسين؛ الكيلاني،محمود. **إدارة امن المعلومات**. الطبعة، 01. عمان. دار الثقافة للنشر والتوزيع، 2015. ص 34

4. الطائي، محمد عبد الحسين؛ الكيلاني،محمود. **المرجع نفسه**. ص 36

حسب التقرير الصادر عن الاتحاد الدول للاتصالات حول اتجاهات الاصلاح في الاتصالات سنة 2010-2011: يعرف الأمن السيبراني: "أنه يُعد مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات إدارة المخاطر وتدريبات وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". [1]

عرف تنظيم الهيئة الوطنية الأمن السيبرانيNCA على أنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها.[2]

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني "فاعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكا لها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث. في حين اعتبر الإعلان الأوروبي الأمن السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".[3]

ويعرف الأمن السيبراني بأنه:" حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير المشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي".[4]

خلاصة لما سبق ذكره فإن الحديث على الأمن السيبراني يقودنا إلى أن:

- الأمن السيبراني هو "عبارة عن مجموعة الوسائل والتنظيمية الإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، الأمن الدفاعي".

---

[1] . الخضر،دلال؛ بن ديلمي،إسماعيل. **المورد البشري خطر أم حصن للمنظمة؟ مدخل إلى أمن المعلومات في ظل الذكاء الاقتصادي**، مجلة الافاق للدراسات الاقتصادية. المجلد، 05. العدد، 01، 2020. ص 126

[2]. الهيئة الوطنية للأمن السيبراني: المملكة على الموقع:https://nca.gov.sa/ar/

[3]. بن عزوز، حاتم. **الأمن السيبراني والجريمة الاليكترونية في الدول ما بعد الحداثية: الولايات المتحدة الأمريكية –نموذجا-**. مجلة الرسالة للدراسات الإعلامية. المجلد، 06. العدد، 02، 2022. ص 582

[4] . الطيطي،خضر مصباح. **أساسيات امن المعلومات والحاسوب**. الطبعة،01. عمان. دار الحامد للنشر والتوزيع، 2010. ص 42

- الأمن السيبراني "هو سلاح استراتيجي بيد الأفراد والحكومة لاسيما أن الحرب السيبرانية أصبحت جزأ لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول، حروب الجيل الخامس".
- الأمن السيبراني "يتضمن إمكانات الحد من الخسائر والأضرار والحيلولة دون وصول إلى خسائر دائمة واحتوائها في أسرع وقت ممكن

2.1.3 الأمن السيبراني وأهميته في المكتبات

تعتبر المكتبة الجامعية مؤسسة عمومية وثقافية تربوية واجتماعية تهدف إلى جمع مصادر المعلومات وتنميتيها وركيزة أساسية من ركائز التعميم في الجامعة حيث تهدف إلى تيسير انتفاع أعضاء التدريس والطلبة بمصادر المعلومات في التكوين الأكاديمي والبحث العلمي، كما تسعى إلى تشجيع البحوث والدراسات المتعمقة بالعمل المكتبي في الجامعة وتنسيق النظام والإجراءات الفنية في المكتبات الجامعية ورفع كفاءة العاملين فيها وتدريبهم على الأساليب المكتبية الحديثة.[1]

كما ترتبط المكتبات الجامعية برؤية المؤسسة الأم؛ وذلك لما تقدمه من دور في رفع مستوى الأداء وخلق قيمة في تعزيز مكانتها وأدوارها لدى المستفيدين وتنمية احتياجاتهم المعلوماتية وتحقيق الأهداف الإستراتيجية للجامعة.[2]

وبالرغم من الفرص التي ترافق استخدام التكنولوجيا الا أن المعلومات تتعرض إلى أشكال متعددة من التهديدات والمخاطر المرتبطة بأمن السيبراني يمكن أن تشمل فقدان البيانات، والهجمات السيبرانية، وانتهاك الخصوصية، الأمر الذي يشكل تحديا لموظفي المكتبات الجامعية وهذا الأمر يتطلب فهما دقيقا للعمليات الجارية في المكتبة ودورة البيانات في النظام والتهديدات المترتبة عنه من خلال الوعي بمفهوم إدارة مخاطر أمن المعلومات وإستراتيجياتها في بيئة المكتبات الجامعية.[3]

ومن هنا تكمن أهمية الامن السيبراني بالنسبة لجميع المكتبات الجامعية في حماية وتسيير وظائفها وخدماتها، لمواجهة المخاطر الداخلية أو الخارجية، وكذا التكنولوجية التي يمكن أن تحدث لبعض العمليات الجارية والأنشطة المستقبلية والتي إذا وقعت تؤثر سلبا على أداء واستمرارية خدماتها وكذا سمعتها لدى جمهور مستنفديها، فضلا على انه يساهم في المحافظة على امن البيانات والمعلومات في المكتبات وسريتها، وذلك من خلال التصدي

---

[1] . رايس، عبد الوهاب؛ صغيري،ميلود. **درجة وعي موظفي المكتبات بمفهوم إدارة مخاطر امن المعلومات في المكتبات الجامعية: دراسة ميدانية بمكتبات جامعة محمد خيضر بسكرة**. مجلة العلوم الإنسانية. المجلد، 24. العدد، 02، 2024. ص 92

[2] . رايس، عبد الوهاب؛ صغيري،ميلود. **المرجع نفسه**. ص 92

[3] . الشوابكة،عدنان عواد.**دور إجراءات امن المعلومات في الحد من مخاطر امن المعلومات في جامعة الطائف**. مجلة الدراسات والأبحاث. المجلد، 11. العدد، 04، 2019. ص 170

للهجمات الخارجية أو الداخلية على شبكة الانترنيت.[1] خاصة مع تحول المكتبات الى استخدام الأنظمة الرقمية والمصادر الالكترونية وتتمثل أهمية الامن السيبيراني في المكتبات فيما يلي:

- حماية البيانات الشخصية والمعلومات الحساسة: وذلك بتوفير أنظمة حماية خاصة بالبيانات والمعلومات الشخصية المتعلقة بالطلاب وأعضاء هيئة التدريس والمستفيدين مثل: (الأسماء، العناوين، أرقام الهواتف، والبريد الالكتروني)، والسجلات الاكاديمية والبحثية، وبيانات تسجيل الدخول الى أنظمة المكتبة.[2]

- حماية الموارد الرقمية: يسعى الأمن السيبيراني إلى حماية الموارد الرقمية في المكتبات الجامعية من خلال توفير مجموعة من الإجراءات والتقنيات التي تضمن سلامة البيانات والمعلومات الحساسة المخزنة في قواعد البيانات الإلكترونية. هذه الموارد تشمل الأبحاث الأكاديمية، الكتب الإلكترونية، الأطروحات العلمية، والدوريات التي تعتبر أصولاً رقمية ثمينة للمكتبة. يعتمد الأمن السيبيراني على تقنيات مثل التشفير لتأمين البيانات أثناء نقلها بين المستخدمين والخوادم، والجدران النارية التي تمنع الهجمات غير المصرح بها، بالإضافة إلى برامج كشف التسلل التي تراقب الأنشطة المشبوهة في الشبكات. كما يتم استخدام أنظمة النسخ الاحتياطي المنتظم لضمان استعادة الموارد في حالة حدوث أي فقدان أو تلف بسبب الهجمات السيبرانية مثل البرمجيات الخبيثة أو هجمات الفدية. من خلال هذه الإجراءات، يتمكن الأمن السيبيراني من حماية الموارد الرقمية، وضمان توافرها الدائم للمستفيدين دون تهديدات تؤثر على جودتها أو أمانها[3].

- ضمان استمرارية الخدمات الالكترونية: بما أن المكتبات تعتمد بشكل كبير على الأنظمة الرقمية والتقنيات الالكترونية لتوفير الخدمات للطلاب وأعضاء هيئة التدريس مثل: الإعارة الرقمية، والوصول الى المقالات العلمية، ومنصات البحث الالكتروني، أي تعطل في هذه الخدمات قد يؤثر بشكل مباشر على الأنشطة الاكاديمية والبحثية، ومن بين هذه التهديدات التي تؤثر على استمرارية الخدمات الالكترونية "الهجمات الموزعة لحجب الخدمة DDOS" التي تشن عن طريق إغراق خوادم المكتبة بعدد هائل من الطلبات مما يؤدي الى تعطلها وعدم القدرة على تقديم الخدمة. والبرمجيات الخبيثة أو الأخطاء البشرية لعدم اتباع الموظفين لإجراءات الأمنية الصحيحة قد يؤدي الى اختراق الأنظمة أو تعطلها.[4]

---

[1] . الشوابكة،عدنان عواد. **المرجع السابق**. ص 171

[2] . فيلالي، أسماء؛شليل، عبد اللطيف، **تهديدات امن المعلومات وسبل التصدي لها**، مجلة البشائر الاقتصادية. المجلد، 04. العدد، 02، 2019. ص100

[3] . محمد عابد، نبيلة. والحداد، أحمد. **متطلبات تحقيق الأمن السيبيراني في المكتبات الجامعية دراسة حالة**. مجلة جامعة البيضاء. المجلد، 04. العدد، 02، 2022. ص 703 – 704

[4] . محمد السنهوري. أحمد. **الأمن السيبيراني في مواجهة الجرائم الغير الأخلاقية**. طبعة، 01. عمان. دار اليازوري العلمية للنشر والتوزيع، 2023. ص 224 - 225

- التصدي للتطور السريع في التهديدات الإلكترونية: فالهجمات السيبرانية تتطور باستمرار من حيث التقنية والأسلوب، لهذا وجود بنية تحتية للأمن السيبيراني يمكن المكتبات من التصدي للهجمات الجديدة مثل البرمجيات الخبيثة وهجمات الفردية.[1]

3.1.3 الأهداف المحورية للأمن السيبراني في المكتبات الجامعية

تُعد المكتبات الجامعية من الركائز الأساسية في العملية التعليمية والبحثية، حيث توفر بيئة غنية بالمصادر الرقمية والخدمات الإلكترونية لدعم الطلاب والباحثين وأعضاء هيئة التدريس. ومع التحول الرقمي الذي تشهده هذه المكتبات، أصبحت تعتمد بشكل كبير على التكنولوجيا والأنظمة الإلكترونية لتوفير الوصول إلى المعلومات بشكل أكثر كفاءة وفعالية.

وتتمثل العلاقة بين الأمن السيبراني والمكتبات الجامعية في الحاجة إلى توفير بيئة آمنة تحمي مصادر المعرفة من التهديدات مثل: الإختراقات، الهجمات الإلكترونية، وتسرب البيانات وغيرها،حيث يساهم ذلك في تعزيز الثقة لدى المستفيدين وضمان استمرارية الخدمات التي تقدمها المكتبات الجامعية، بما يدعم تحقيق أهدافها التعليمية والبحثية. بالتالي يُعتبر الاستثمار في الأمن السيبراني ضرورة إستراتيجية لضمان حماية البيانات الرقمية والحفاظ على إستدامة دور المكتبات الجامعية في المجتمع الأكاديمي.[2]

ويمكن توضيح الأهداف الرئيسية للأمن السيبيراني في بيئة المكتبات الجامعية في مايلي:

1.3.1.3تأمين النظام والتطبيقات:

ويقصد بأمن النظام والتطبيقات حماية أنظمة التشغيل المعتمدة في إدارة منظومة الحواسيب والعمل على تقليل أو منع محاولات التلاعب بالثوابت أو المفاتيح المنطقية التي تتحكم في عملية السيطرة على تنفيذ البرمجيات ونظم التشغيل.[3]

---

[1] . محمد السنهوري. أحمد. **المرجع نفسه**. ص 225

[2] . الحمامي، علاء حسين؛ العالي، سعد عبد العزيز. **تكنولوجيا أمنية المعلومات وأنظمة الحماية**. طبعة، 01. عمان: دار وائل للنشر والتوزيع، 2007، ص 100 - 103

[3]. صادق، دلال؛ الفتال، حميد ناصر. **أمن المعلومات**. طبعة، 01. عمان. دار البازوزي العلمية للنشر والتوزيع، 2008. ص 99

وبناء على ذلك يمكن تحديد مستويات الحماية طبقا لسرية وخطورة البيانات من خلال وضع سياسات مسبقة مبنية على التنبؤ بجميع الاحتمالات الواردة، ووضع الخطط وتوفير التقنيات والوسائل.إذ يمكن حماية النظم والتطبيقات قبل الولوج إليها والعبث بها. لتحقيق ذلك لابد من إتباع مجموعة من الإجراءات وهي كمايلي:

1. القدرة على تحديد مصادر التهديد أولا، ثم معرفة مدى نجاح مصدر التهديد في الإضرار بالنظام من خلال تحديد نقاط الضعف الموجودة به. وبعد ذلك يتم العمل على تطوير النظام تماشيا مع طبيعة كل المخاطر المهددة ووضع مختلف السبل للحد منها قبل وقوعها.
2. مضادات الفيروسات: ويقصد بها البرمجيات التي تستخدم لمنع وإكتشاف وإزالة البرمجيات الخبيثة بما في ذلك الحاسب والديدان، وأحصنة طروادة وملوثات مقاطع التحميل، والكود التخريبي وغيرها. وهي عبارة عن أدوات برمجية تستخدم من أجل القيام بعمليات الهجوم الفعال والمضر للنظام، والعلاج الناجح للفيروسات يكون باتخاذ إجراءات الأمن السيبيراني[1].
3. البريد الالكتروني: يعتبر البريد الإلكتروني من وسائط الإتصال الموثوقة بالنسبة لمستخدميه في المكتبات الجامعية، إذا كان هناك أشخص يرغبون في الحصول على فائدة أكبر من إستخدام البريد الاليكتروني كالصفات المتطورة لبرمجيات البريد الإلكتروني فإن مجرد فتح رسالة واردة تعد تجربة مخيفة.فالمرسل يستطيع أن يرسل ملف أو عنوان أو اسم يحتوي على ملف مغشوش قد يؤدي إلى هجوم خارجي على قاعدة النظام.
4. حماية خصوصية البيانات:إن حرية تداول المعلومات وحرية التعبير التي تنص عليهما المادة 19 من الإعلان العالمي لحقوق الانسان، مبدآن آساسيان في مهنة المكتبات والمعلومات. وتعد الخصوصية جزء لا يتجزأ من هذه الحقوق والخصوصية في المكتبات الجامعية ومراكز المعلومات ضرورية عند التعامل معهما، لهذا نجد من الأهداف التي يسعى له الأمن السيبيراني هو تحقيق هذه الخصوصية.[2]

---

[1] . عقابو، خالد؛ بومعرافي، بهجة. **حماية الكيانات الرقمية وضمان استمراريتها من خلال استراتيجيات امن المعلومات بالمستودعات الرقمية الجامعية: مستودع جامعة محمد خيضر بسكرة نموذجا**. مجلة المعيار. المجلد، 27. العدد، 03، 2023. ص 761 - 762

[2] . عقابو، خالد. بومعرافي، بهجة. **المرجع نفسه**. ص 750

كما تتيح لمستخدمي المكتبة استخدام المعلومات والأفكار والوصول اليها والاطلاع عليها دون خوف من الاحراج او العقوبة أو انتهاك الخصوصية. حيث يمكن لانتهاك الخصوصية ان يؤثر سلبا على رغبة مستخدمي المكتبة في زيارة المكتبات ومراكز المعلومات، مما يؤثر بشكل كبير على حرية الوصول إلى الأفكار والتعامل مع المكتبة بشكل خاص خوفا من الانتهاك. وعليه نجد الكثير من الدراسات اتفقت على توفر طرق لتأمين البيانات المستفيدين وذلك عن طريق تخصيص حاسبات آلية تقوم بمسح التعاملات التي تمت عليها تلقائيا، والقيام بإجراءات تدقيق الخصوصية مع التوازن والتوفيق بين زيادة الوصول للمعلومات والمحافظة على خصوصية المستفيدين.[1]

2.3.1.3التصدي للهجمات وحوادث أمن المعلومات:

تتعرض المكتبات الجامعية مثل غيرها من المنشآت العامة والخاصة إلى مخاطر وحوادث مختلفة، وتظهر مجموعة المخاطر في العديد من الأشكال مثل: الهجوم السيبراني، وسرقة المعلومات، وتخريب العمل. الأمر الذي يؤثر سلبياعلى المؤسسة. ولذلك على المكتبات الجامعية أن تقوم بتفعيل مجال الأمن السيبيراني المتغير والمتسارع من خلال مايلي:

1. تطبيق الضوابط والمتطلبات التي تحقق أمن المعلومات في منشأتها.
2. العمل على تخريج مهنيين بارعين لفهم العمليات التي تؤثر على أمن البيانات.
3. تحديد الثغرات الأمنية وإصلاحها.
4. حماية الأنظمة الرقمية والشبكات والمعلومات من التهديدات والهجمات التي قد تؤثر على سلامتها وسرية بياناتها.[2]
5. توفير آليات متطورة لحماية أنظمة المعلومات والشبكات من الهجمات الإلكترونية مثل: الفيروسات، والبرمجيات الخبيثة، وهجمات التصيد الاحتيالي وغيرها..، يتم ذلك من خلال استخدام جدران الحماية وأنظمة كشف التسلل ID.[3]

---

[1]. السعيد، سلوى. لبيب، ندىمصطفي. **حماية خصوصية بيانات المستفيدين في المكتبات الأكاديمية: مراجعة علمية للإنتاج الفكري**. مجلة الدولية لعلوم المكتبات والمعلومات. المجلد، 10. العدد، 03، 2023. ص 369

[2]. بن عبد الله الهزائي، نورة. **ضوابط ومتطلبات تطبيق الأمن السيبيراني لحماية البيانات في جامعة الأميرة نورة**. مجلة مكتبة الملك فهد الوطنية. المجلد 02. العدد، 28، 2023. ص 66

[3]. الغنيمي، أشرف. **نظم الحماية من قراصنة الكمبيوتر**. طبعة، 01. القاهرة. دار الفاروق للنشر والتوزيع، 1997. ص 164

4.1.3تأثير الأمن السيبيراني على الخدمات المكتبية الرقمية:

عرف التحول الرقمي العديد من التطورات والتغييرات في بيئة المكتبات وخصوصا المكتبات الجامعية، ولطالما حرصت المكتبات الجامعية على مواكبة التحولات الجديدة من خلال إتاحة خدمات إلكترونية للمستفيدين لتسهيل الوصول إلى المعلومات المطلوبة في أقل وقت وجهد. وبما أن الخدمات الإلكترونية للمكتبات الإلكترونية متاحة في الفضاء السيبراني فإن تحقيق الأمن السيبراني على الخدمات المكتبية الإلكترونية؛ يعد أحد أبرز التحديات التي تواجهها المكتبات الجامعية لما له من تأثيرات إيجابية وسلبية على المؤسسة، ومما سبق ذكره يظهر تأثير الأمن السيبراني على الخدمات المكتبية الرقمية في المكتبات الجامعية في مايلي:

1. **السرية:** من بين التأثيرات الإيجابية التي يقدمها الأمن السيبيراني اتجاه الخدمات المكتبية هي ضمان أن البيانات والمعلومات المخزنة أو المتبادلة في أنظمة المكتبة الرقمية لا يمكن الوصول اليها أو الاطلاع عليها إلا من قبل الأشخاص المصرح لهم. إضافة إلى تأمين الوصول، بحيث يمنع أي شخص غير مصرح له من الوصول الى المعلومات الحساسة مثل البيانات الشخصية للمستخدمين، محتويات الكتب أو الأبحاث الرقمية المحمية، أو السجلات الداخلية للمكتبة.وعليه نجد أنإستخدام الأمن السيبيراني له تأثير كبير في ضمان سرية البيانات خاصة أثناء نقلها عبر الشبكات، مثل: عمليات البحث أو استعارة الكتب الرقمية، بحيث لا يمكن اعتراض البيانات أو قراءتها من قبل أطراف غير مخولة[1].
2. **إستمرارية الخدمة:** تعني ضمان بقاء المكتبة الرقمية متاحة وآمنة أمام المستخدمين على مدار الساعة، مما يؤثر بشكل إيجابي في تقديم تجربة موثوقة ودائمة دون تأثير سلبي للتهديدات السيبرانية. ويمكن توضيح ذلك في النقاط الآتية:[2]

[1] . الحوش، محمود أبو بكر. **التقنية الحديثة في المعلومات والمكتبات**. طبعة، 01. عمان. دار الفجر للنشر والتوزيع، 2022. ص 103

[2] . داود، مسعود. **الخدمات الرقمية للمكتبات العربية في ظل جائحة كوفيد 19 المكتبة المركزية بجامعة الجزائر 02 أنموذجا – دراسة تحليلية**. دراسات نفسية وتربوية. المجلد، 14. العدد، 02، 2021. ص 580

- حماية الأنظمة من الأعطال الناتجة عن الهجمات السيبرانية: من خلال تطبيق أنظمة الأمن السيبراني القوية، يمكن للمكتبة التصدي لهذه الهجمات والحفاظ على استمرارية خدماتها مثل البحث، تنزيل الكتب، والوصول إلى قواعد البيانات.
- الحد من التوقف غير المتوقع: الأعطال التقنية التي قد تنتج عن فيروسات أو برامج ضارة تؤدي إلى توقف الخدمات. يوفر الأمن السيبراني إستراتيجيات مثل التحديث الدوري، الفحص المستمر، والتصدي الفوري للتهديدات لتجنب هذه الأعطال وضمان بقاء الخدمات متاحة على مدار الساعة.[1]
- ضمان الوصول المستمر للمستخدمين: إستمرارية الخدمات تعني أن المستخدمين يمكنهم الوصول إلى المنصات الرقمية للمكتبة في أي وقت ومن أي مكان دون القلق من إنقطاع الخدمة أو فقدان البيانات، مما يوفر حماية للخوادم والأنظمة ويتيح تجربة مستخدم مستقرة.[2]
- إستعادة الخدمة بسرعة في حالات الطوارئ: حتى في حال وقوع هجوم سيبراني أو عطل كبير، يمكن لأنظمة الأمن السيبراني المتقدمة أن تضمن إستعادة الأنظمة والخدمات بسرعة.
- تعزيز الكفاءة التشغيلية: المكتبة الرقمية التي تعتمد على إجراءات أمن سيبراني فعالة تقلل من وقت التوقف والإصلاحات، مما يعزز من كفاءة العمليات ويضمن استمرارية العمل دون تأخير. [3]
- التكامل مع الإبتكارات التكنولوجية: إستخدام تقنيات الأمن السيبراني المتطورة يمكن للمكتبات الرقمية تبني خدمات جديدة (مثل الذكاء الاصطناعي أو البحث الصوتي) دون القلق من تأثيرها على إستمرارية الخدمة.[4]

---

[1] . داود، مسعود. **المرجع السابق**. ص 581

[2] . داود، مسعود. **المرجع نفسه**. ص 582

[3] . محاجبي، عيسى؛ زيرام، بهية. **إدارة الكفاءات في المكتبات الجمعية الجزائرية باعتماد مواصفة ايزو 9001: المكتبة المركزية لجامعة الجزائر 02 أبو القاسم سعد الله أنموذجا**. مجلة العلوم الاجتماعية والإنسانية. المجلد، 11. العدد، 02، 2021. ص 1016

[4]. كادي، زين الدين. **إجراءات الأمن والوقاية من الجرائم الاليكترونية في المكتبات ومراكز المعلومات**. مجلة الإشارة. المجلد، 03. العدد، 01. ص 65

- **الثقة والمصداقية:** ويقصد بذلك تعزيز ثقة المستخدمين بالمكتبة وخدماتها مما يجعلها مصدرا موثوقا للمعلومات وبالتالي عندما توفر المكتبة الرقمية تدابير قوية للأمن السيبيراني، يشعر المستخدمون بالإطمئنان، ذلك أن معلوماتهم الشخصية مثل: (الأسماء، الحسابات، السجلات، بيانات البحث) محمية من التسريب أو السرقة. هذا ما يعزز إحساسهم بالأمان أثناء استخدام الخدمات المكتبية الرقمية. وإقبالهم على الخدمات الجامعية بشكل أكبر والتفاعل مع المكتبة الرقمية سواء بالاستعارة، التسجيل، أو حتى مشاركة معلوماتهم الشخصية مع النظام، خاصة عندما تلتزم المكتبة الرقمية بتطبيق معايير وقوانين حماية المعلومات فان ذلك يظهر جديتها في حماية حقوق المستخدمين مما يزيد من مستوى الثقة بها. [1]
- **الابتكار وتقديم خدمات جديدة:** الأمن السيبراني له تأثير كبيرا في تعزيز جودة الخدمات التي تقدمها المكتبات الرقمية، حيث يوفر بيئة آمنة لحماية البيانات والمعلومات الشخصية للمستفيدين من المخاطر الإلكترونية مثل القرصنة أو تسريب البيانات. بفضل تقنيات الأمن السيبراني، تستطيع المكتبات الرقمية تقديم خدمات مبتكرة تلبي إحتياجات المستخدمين، مثل الوصول الآمن إلى قواعد البيانات والمصادر الإلكترونية عبر التحقق الثنائي، وتخصيص المحتوى بناءً على اهتمامات المستخدمين دون المساس بخصوصيتهم. بالإضافة إلى ذلك، تتيح أنظمة الأمن المتطورة إمكانية تطوير منصات تعليمية تفاعلية وخدمات استشارية إلكترونية، مما يعزز من تجربة المستخدمين ويزيد من ثقتهم في استخدام المكتبة الرقمية. بالتالي، يشكل الأمن السيبراني دعامة أساسية لتمكين المكتبات من التوسع في خدماتها وإبداع حلول جديدة تلائم التطور الرقمي.[2]
- **الأمن السيبراني لا يقتصر فقط على حماية المعلومات،** بل يسهم أيضًا في تطوير البنية التحتية الرقمية للمكتبات، مما يفتح المجال لتقديم خدمات جديدة ومبتكرة. على سبيل المثال، من خلال استخدام تقنيات التشفير وحماية البيانات، يمكن للمكتبات توفير منصات استعارة إلكترونية آمنة تتيح للمستفيدين تحميل الكتب الرقمية أو الوصول إلى المقالات الأكاديمية دون القلق بشأن انتهاك حقوق الملكية الفكرية، كما يتيح الأمن السيبراني للمكتبات إمكانية تبني تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة لتخصيص المحتوى وفقًا لاحتياجات وتفضيلات كل مستخدم، مما يعزز التفاعل بين المكتبة والمستفيدين.[3]

---

[1] . الغنيمي، أشرف. **المرجع السابق**. ص 168

[2] . قارح، سماح. تسامده، حسان. **الابداع والابتكار في نظم وتكنولوجيا المعلومات: دراسة ميدانية لعينة من مكتبات الوسط الجزائري**. المجلة الجزائرية للعلوم الاجتماعية والإنسانية. المجلد، 09. العدد، 02، 2021. ص 48 -50

[3] . قارح، سماح. تسامده، حسان. **المرجع نفسه**. ص 51

- **توفر حلول الأمن السيبراني حماية** للمعاملات المالية المتعلقة بالخدمات المدفوعة، مثل الاشتراكات أو شراء الكتب الإلكترونية، مما يزيد من ثقة المستخدمين في التعامل مع المنصات الرقمية للمكتبة. كما يمكن للأمن السيبراني دعم المكتبات في بناء أنظمة تعاون آمنة بين المؤسسات الأكاديمية والبحثية، مما يعزز من تبادل المعرفة والموارد.[1]
- **الحفاظ على سمعة المكتبة الرقمية**: يُعد الأمن السيبراني عنصرًا حيويًا في الحفاظ على سمعة المكتبة الرقمية، حيث يضمن حماية البيانات والمعلومات التي تحتويها المكتبة من التهديدات السيبرانية مثل الاختراقات والهجمات الإلكترونية. توفر إجراءات الأمن السيبراني بيئة آمنة للمستخدمين لحفظ بياناتهم الشخصية وسجل أنشطتهم داخل المكتبة الرقمية، مما يعزز ثقتهم في استخدام خدماتها. كما أن الحماية من تسرب البيانات أو التلاعب بها تسهم في الحفاظ على مصداقية المكتبة، وضمان توفير مصادر المعلومات دون انقطاع أو مخاطر. علاوة على ذلك، يُظهر تطبيق أنظمة الأمن السيبراني التزام المكتبة بأعلى معايير السلامة التقنية، ما يدعم صورتها كمنصة احترافية جديرة بالثقة لدى الباحثين والقراء والمجتمع الأكاديمي.[2]

إضافة إلى ما سبق، فإن الأمن السيبراني يساهم في تعزيز استدامة المكتبة الرقمية من خلال توفير حماية متكاملة لأنظمتها التقنية، مما يقلل من مخاطر التعطيل أو فقدان البيانات. يساعد ذلك المكتبة في تقديم خدماتها بكفاءة واستمرارية دون انقطاع، وهو ما يعكس التزامها بجودة الخدمة. علاوة على ذلك، يعمل الأمن السيبراني على التصدي للهجمات التي قد تستهدف تعطيل أنظمة المكتبة أو تشويه سمعتها، مثل هجمات الفدية أو البرمجيات الخبيثة. عندما تطبق المكتبة تدابير أمنية صارمة مثل التشفير، وأنظمة الحماية المتقدمة، وبرامج مكافحة الفيروسات، فإنها تعزز من قدرتها على التصدي لهذه التهديدات.[3]

والأمن السيبراني لا يحمي فقط المعلومات الرقمية، بل يعزز أيضًا من التفاعل الإيجابي بين المستخدمين والمكتبة. عندما يشعر المستخدمون بالأمان أثناء تصفحهم للمصادر الرقمية أو تحميلهم للملفات، فإن ذلك يزيد من رضاهم وولائهم للمكتبة. وفي المقابل، فإن أي خرق أمني قد يؤثر سلبًا على سمعة المكتبة، ويؤدي إلى فقدان الثقة بها، مما يجعل الاستثمار في الأمن السيبراني ضرورة استراتيجية وليس خيارًا. [4]

---

[1] . بن السبتي، عبد المالك. **تكنولوجيا المعلومات في المكتبات الجزائرية بين الرغبة والتغيير والصعوبات. مجلة علوم الاعلام والتكنولوجيا**. المجلد، 14. العدد، 01، 2004. ص 14

[2] . بن االسبتي، عبد المالك. **المرجع السابق**، ص 16

[3] . جلول، نادية. **المكتبات الرقمية في عصر المعلوماتية بين التطوير والتعميم**. مجلة النص. المجلد، 03. العدد، 01، 2021. ص 60

[4] . جلول، نادية.**المرجع نفسه**. ص 65

لكن بالرغم من الاثار الإيجابية لأمن السيبيراني في المكتبات الجامعية إلا أننا لا ننفي أنه سلاح ذو حدين، فقد تواجه المكتبات الجامعية العديد من التحديات في ظل تزايد الاعتماد على التكنولوجيا والأمن السيبراني لحماية المعلومات الرقمية والمحتوى الأكاديمي. بالرغم من أن الأمن السيبراني يعد عاملاً أساسياً للحفاظ على سلامة البيانات وحمايتها من الهجمات الإلكترونية، إلا أن تطبيقات الأمن السيبراني قد تترتب عليها بعض الآثار السلبية التي تؤثر في سير العمل داخل المكتبات الجامعية. ومن بين الأثار السلبية هي زيادة التهديدات الإلكترونية التي قد تهدد سلامة المحتوى الأكاديمي المخزن على أنظمة المكتبة. الهجمات الإلكترونية مثل الفيروسات، والبرمجيات الخبيثة، وعمليات الاختراق قد تؤدي إلى فقدان البيانات القيمة، مما يعطل الوصول إلى الكتب الإلكترونية، قواعد البيانات، والبحوث العلمية. في مثل هذه الحالات، يمكن أن تتأثر مصداقية المكتبة وقدرتها على تقديم خدمة فعالة للطلاب والباحثين.[1]

- تسبب تعقيد تقنيات الأمن السيبراني في صعوبة إدارة المكتبة بشكل يومي. فالمكتبات الجامعية غالبًا ما تفتقر إلى الموظفين المدربين على التعامل مع تقنيات الأمان المعقدة، مما قد يؤدي إلى مشكلات في التنفيذ والصيانة المستمرة للأنظمة الأمنية. كما أن هذه التقنية المتقدمة قد تكون مكلفة، مما يترتب عليه تأثير سلبي على ميزانية المكتبة، حيث يتعين تخصيص مبالغ كبيرة لهذه الإجراءات الأمنية على حساب تطوير وتحسين الخدمات الأخرى مثل توسيع الموارد الإلكترونية أو تحسين بيئة العمل للطلاب.[2]

وفي الأخير يمكن القول أن توفير الأمن السيبراني لحماية المعلومات الرقمية في المكتبات الجامعية ضروري، وتطبيقه يحتاج إلى توازن دقيق بين الأمان وسهولة الوصول إلى الخدمات، مع ضرورة تخصيص موارد تدريبية وتقنية لموظفي المكتبة لضمان تنفيذ إستراتيجيات الأمان بفعالية.

2.3 أنواع مخاطر الأمن السيبيراني في المكتبات الجامعية:

شهدت المكتبات خلال السنوات الأخيرة الماضية موجة من التغيرات والتطورات التي ساعدت في رفع أدائها والارتقاء بخدماتها وتحقيق أهدافها، إلا أن ربط المكتبات بالعالم الخارجي عبر شبكة الإنترنت أدى إلى تعرضها للكثير من المخاطر والهجمات الإلكترونية التي تهدد أمن وسلامة وسرية المعلومات على المكتبات والأجهزة والتطبيقات والشبكات المتوافرة بها، ومن ثم ينبغي على المكتبات الإهتمام بتأمين المعلومات لحمايتها من الاختراق والهجمات الضارة التي تهدد نظام المكتبة، ومن بين الهجمات الضارة التي قد تهدد الأصول المعلوماتية والنظم الآلية وتعمل على تدميرها أو إتلافها هي:

---

[1] . بن السبتي، عبد المالك. **المرجع السابق**. ص 16-17

[2] . بعنوني، ليلي. **التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا**. مجلة دراسات الدفاع والاستشراف. المجلد، 08. العدد،02، 2021. ص 12 - 13

1.2.3الهجمات الإلكترونية:

يستهدف هذا النوع أنظمة الحاسب الآلي والتطبيقات والبرامج وملفات البيانات والمعلومات؛ حيث تتسلل لها من خلال إستغلال الثغرات الأمنية أو نقاط الضعف وتسمح لغيرالمفوضين باقتحام الأجهزة والتطبيقات والبرامج وإتلافها أو إساءة استخدامها.وهذه الهجمات الإلكترونية قد تكون موجهة للفرد أو مؤسسات بعينها للإختراق الأصول المعلوماتية الخاصة بها. وفيما يلي نذكر أنواع التهديدات الإلكترونية الأكثر انتشار وحداثة[1]وهي:

1.1.2.3 الفيروسات:

هو برنامج تخريبي تتم برمجته على أيدي محترفين بحيث يحدث هذا البرنامج خلل في خصائص الملفات التي يستهدفها، ليجعلها تحت سيطرة المبرمج من خلال حذف جميع مستندات هذا الملف أو تخريبها أو التعديل عليها، وتكون الغاية من هذ البرامج تخريب أجهزة الحاسوب الخاصة بالمستخدمين، وكما قد يكون الهدف منه الحصول على ملفات وبيانات من جهاز مستخدم ما، والتعرض لهجمات فيروسية يعتبر من نوع هجمات سيبرانية تؤدي إلى تعطل الخدمة لذا يجب الحماية منه.[2].

تنتقل الفيروسات في الحاسوب بطريقتين رئيسيتين:

أ.**العدو المباشرة**Infector Direct: يغزو الفيروس ملفات الحاسوب وعندما يتم تشغيل أو استخدام أحد هذه الملفات فإن الفيروس يبدأ نشاطه وإنتشاره، وينتقل بين الملفات الموجودة على جهاز الحاسوب، فور انتقال العدو إلى ملف فإنه يتم تحميله ونقله إلى الذاكرة تلقائيًا ومن ثم تشغيله.

ب.**العدو غير المباشرة**Infector Indirect: ينقل البرنامج المصاب بالفيروس إلى ذاكرة جهاز الحاسوب فور بدء تشغيل الملف المصاب، ينفذ الحاسوب أوامر الملف الأصل ثم ينقل الإصابة ويتم تحميله إلى الذاكرة. يتوقف هذا النوع من الإنتشار في حال فصل التيار الكهربائي عن جهاز الحاسوب أو إعادة التشغيل، مثل ملف وورد مصاب[3].

---

[1]. كاوجة، محمد الصغير. **الهجمات السيبرانية بين الواقع وسبل المواجهة**. مجلة الرسالة للدراسات الإعلامية. المجلد، 06. العدد، 03، 2022. ص 110- 112

[2] . ميلود، ليفة. **أحكام الاتلاف الفيروسي للبرامج والبيانات الاليكترونية**. مجلة البحوث والدراسات. المجلد، 13. العدد، 02، 2016. ص 65

[3] . كادي، زين الدين. **المرجع السابق**. ص 70

تقسم الفيروسات إلى نوعين رئيسيين هما فيروس الماكرو Macro virus، وفيروس قطاع التشغيل Boot sector virus وكل من النوعين يختلف في طريقة إصابته لأجهزة الحاسب، كما يختلف في طريقة تأثيره عليها:

1.1.1.2.3فيروس الماكرو: عبارة عن برنامج صغير مكتوب باستخدام لغة برمجة داخلية للتطبيقات مثل فيجوال بيسيك للتطبيقات، ويقوم فيروس الماكرو على عمل نسخ من نفسه بداخل الملفات المنشأة باستخدام البرامج التطبيقية مثل برامج Word,Win Word ويعمل الماكرو عند فتح أو إغلاق الملف أو عند حفظ ملف أو أثناء تشغيل البرنامج.

2.1.1.2.3فيروس قطاع التشغيل: تتركز هذه الفيروسات في قطاع التشغيل لأقراص الحاسب الآلي، ولا تحتاج كالنوع السابق الى ملفات للدخول إلى الجهاز حيث يصاب الجهاز بالفيروس عند محاولة تشغيله من خلال قرص مصاب بالفيروس. وبتشغيل جهاز الحاسب ينتقل الفيروس الى الذاكرة ويحدث عدوى لكل قرص يتم تشغيله[1] على الجهاز، ويقوم الفيروس بكتابة نسخة من نفسه على كل قرص سليم ليصيبه. ويسبب هذا النوع من الفيروسات ظهور رسالة خطأ عند تشغيل الحاسب الآلي بالعدوى مثل: missing operating system. وعلى الرغم من أن الانتشار بالنسخ التلقائي يعد أحد السمات المميزة للفيروسات، إلا أن مصطلح فيروس يطلق أيضاً على برامج أخرى مصممة لإلحاق الأذى بالحاسبات وهي البرامج الخبيثة[2].

2.1.2.3البرمجيات الخبيثة:

وهي برامج أو شيفرات برمجية ضارة تصمم بهدف الحاق الضرر بالأجهزة أو الشبكات أو البيانات، أو لاختراقها واستغلالها بطريقة غير مشروعة. وتستخدم البرمجيات الخبيثة من قبل المهاجمون لتحقيق أهداف متعددة، مثل سرقة المعلومات، التجسس، وتعطيل الأنظمة والخدمة، أو تحقيق مكاسب مالية[3]. ومن بين أنواع البرمجيات الخبيثة:

---

[1]. العيداني، محمد. **التهديدات السيبرانية وجرائم المعلومات**. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المجلد، 13. العدد، 01، 2024. ص 20 -23

[2]. العيداني، محمد. **المرجع نفسه**. ص 20 -23

[3]. بوخنفر، زوليخة. **إدارة الهوية الرقمية واشكالات السمعة والخصوصية والاختراق: العملاقة على الويب. الشبكات المعلوماتية**. مجلة الرقمنة للدراسات الإعلامية والاتصالية. المجلد، 03. العدد، 01، 2023. ص 70

1.2.1.2.3أحصنة طروادة: Trojans horses

هي برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الأذى بالنظام على الرغم من أنه في ظاهره يبدو كأنما يؤدي أعمالاً عادية، فهي توحي للمستخدم بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملاً آخر تخريبي في الغالب، فتقوم أحياناً بالتجسس ومتابعة كل ما يتم عمله من إجراءات أو تسجيله من بيانات على الجهاز المصاب بها، وتقوم أحياناً أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أو مسحها أو ما سوى ذلك. ولا تتمكن أحصنة طروادة من نسخ نفسها والالتصاق بالبرامج الأخرى ولكنها تؤدي عملاً معيناً تم تصميمها من أجله.

2.2.1.2.3القنابل المنطقيةLogic Booms:

هي من أنواع أحصنة طروادة، وتعمل القنابل المنطقية عند حدوث شرط منطقي محدد مثل بلوغ الموظفين عدداً معيناً أو رفع إسم أحد الموظفين من كشف الرواتب، أو كتابة كلمة معينة، أما القنابل الموقوتة فتعمل وفقاً لتوقيت معين مثل ساعة محددة أو يوم محدد[1].

3.2.1.2.3برامج الطوفان:

وهي تتمثل في مجموعة كبيرة جداً (مئات أو ألوف) من الرسائل التي تصل من جهات غير معروفة إلى الشبكة عن طريق البريد الإلكتروني أو عن طريق برامج ICQ، وهي بدون شك تسبب إزعاجاً كبيراً حتى وإن كانت لا تسبب ضرر.[2]

4.2.1.2.3برامج الخداع:

هذا النوع من البرامج تؤدي إلى تضليل مستقبل المعلومات حيث يبدو أنها مرسلة من جهة معينة في حين أنه في الواقع مرسلة من جهة أخرى؛ الأمر الذي يسمح بدخول المعلومة إلى الشبكة ويجعل مستقبلها يتعامل معها دون معرفة هوية مرسلها الحقيقي.[3]

---

[1] . حميل، مصطفى. **السيادة الرقمية: التحديات والحلول الهيكلية**. مجلة رقمنه للدراسات الإعلامية والاتصالية. المجلد، 02. العدد، 03، 2022. ص 50 – 52

[2] . حميل، مصطفى. **المرجع نفسه**. ص 53

[3]. العيداني، محمد. **المرجع السابق**. ص 25

5.2.1.2.3باب الفخ أو المصيدة:

هذا البرنامج يطلق عليه أيضاً الأبواب الخلفية Backdoors، ويمثل كود يوضع عمداً عند البرمجة لتجاوز نظم الحماية في البرنامج. وهو يسهل على المبرمج الدخول إلى البرنامج والتعديل فيه دون الحاجة إلى اتباع الخطوات التقليدية لذلك. وعادةً يتم حذف أبواب الفخ بعد الانتهاء من جميع الاختبارات الخاصة بالبرنامج، ولكن في بعض الأحيان تترك تلك الأبواب سواء بقصد أو بدون قصد. وقد يكتشف البعض تلك الأبواب ويستغلها لأغراض تخريبية للتجسس وانتهاك سرية البيانات أو لزرع الفيروسات.[1] برامج الفدية:

تعد أكثر أنواع البرامج الضارة ربحية، يقوم فيها المهاجم بتنفيذ سلسلة من الإجراءات التي تعمل على تشفير ملفات كمبيوتر الضحية أو النظام بأكمله؛ ثم يطالب بدفع مقابل مادي بالدولار أو أي عملة أخرى لفك التشفير أو الرمز.[2]

2.2.3تهديدات التسريب والسرقة الإلكترونية:

ظاهرة السرقة العلمية أصبحت من بين أكثر الظواهر انتشارا في الأوساط الجامعية، وزاد انتشارها بشكل رهيب بفضل شبكة الانترنيت. وذلك عن طريق:

1.2.2.3تسريب المعلومات والبيانات الشخصية:

تسريب المعلومات الشخصية في المكتبات الجامعية يُعَدّ من أخطر التهديدات التي قد تواجه هذه المؤسسات، حيث تعتمد المكتبات على قواعد بيانات واسعة تشمل معلومات شخصية للطلاب وأعضاء هيئة التدريس والموظفين، مثل الأسماء، أرقام الهويات، عناوين البريد الإلكتروني، وأحياناً السجلات الأكاديمية. قد يحدث التسريب نتيجة ثغرات أمنية في أنظمة المكتبة الإلكترونية، هجمات سيبرانية مثل القرصنة، أو بسبب إهمال العاملين في حماية البيانات الحساسة. وبالتالي تسريب هذه المعلومات يمكن أن يؤدي إلى مخاطر جسيمة مثل انتحال الهوية، الاحتيال المالي، أو التلاعب بالبيانات الأكاديمية. علاوة على ذلك، فإن هذه الحوادث قد تؤثر على سمعة المكتبة وثقة المستخدمين فيها، مما يضعها في مواجهة تحديات قانونية وأخلاقية.[3]

---

[1] . العيداني، محمد. **المرجع نفسه**. ص 27

[2] . كاوجة، محمد الصغير. **المرجع السابق**. ص 115

[3] . بوقرص، ساعد. **المرجع السابق**. ص 63

2.2.2.3تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية:

ذلك عن طريق شن هجمات إلكترونية في الشبكة المعلوماتية، بقصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية الخاصة بالمكتبة، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، فعملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة بإدارة المكتبة ببرامج شبكة الانترنيت، وهي عملية تتم من أي مكان في العالم دون الحاجة الى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية.[1]

ومن الممكن تصور هجوم اليكتروني على أحد المواقع الالكترونية بقصد تدميرها وشلها عن العمل أو تعطيل الخدمة. حيث بإمكان شن هجوم مدمر لأغلاق المواقع الحيوية التي تخص المكتبات الجامعية على الشبكات المعلوماتية، وإلحاق الشلل بالأنظمة. بحيث يؤدي توقفها عن العمل الى تحقيق اثار سلبية على بيئة المكتبة الجامعية.

3.2.2.3التجسس الإلكتروني:

يشكّل تهديدًا كبيرًا على المكتبات الجامعية، حيث تعتمد هذه المكتبات بشكل متزايد على النظم الرقمية لتقديم خدماتها وإدارة مواردها. يشمل هذا التهديد محاولات لاختراق الأنظمة للحصول على بيانات حساسة، مثل معلومات الطلاب والباحثين، وسرقة الأبحاث أو المواد الرقمية المحمية. قد يُستغل التجسس الإلكتروني في تعطيل الوصول إلى الموارد، مما يؤثر سلبًا على العملية التعليمية والبحثية. إضافة إلى ذلك، يمكن أن تستخدم الجهات الخبيثة تقنيات مثل البرمجيات الضارة أو التصيد الإلكتروني للوصول إلى أنظمة المكتبات أو تدميرها. [2]

4.2.2.3إتلاف المعلومات وتعديلها:

وهي هجمات تهدف الى الوصول للمعلومات التي تخص نظام المكتبة عبر شبكة الانترنيت بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة له. والقيام بعملية تعديل البيانات الهامة التي تخص الطلبة أو الأساتذة أو الموظفين أو مقال بحثية أو مشاريع مستقبلية وغيرها دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة، وقد تؤدي الى نتائج كارثية خاصة إذا تمثلت البيانات في معلومات الشخصية للمكتبة ونظامها، ومن بين النتائج التي من الممكن أن تحصل على سبيل المثال فقدان البيانات وصعوبة استرجاعها، والتلاعب غير

---

[1]. السنهوري، محمد أحمد. **المرجع السابق**. ص 202 -203

[2]. شتا عبد السلام علي، ابتسام. **تأمين المعلومات بمكتبات جامعة الأزهر: المكتبة المركزية نموذجا**. أطروحة لنيل شهادة الدكتوراه. كلية الدراسات الإنسانية، قسم الوثائق والمكتبات والمعلومات: تخصص الوثائق والمكتبات والمعلومات. جامعة الأزهر. القاهرة، مصر، 2023. ص 223

المصرح به بمحتوى المصادر المتوفرة في المكتبة حيث يتم تغيير النصوص وإدخال معلومات خاطئة مما يهدد مصداقية وشفافية المكتبة الجامعية.[1]

5.2.2.3هجمات الأنظمة السحابية :

هجمات الأنظمة السحابية على المكتبات الجامعية تمثل تحديا كبيرا لأنها تستهدف البنية التحتية التي تستخدم لتخزين وإدارة كميات ضخمة من البيانات الرقمية، بما ذلك قواعد البيانات الأكاديمية، الأطروحات، المقالات العلمية، والمصادر التعليمية الأخرى. تعتمد المكتبات الجامعية بشكل متزايد على الخدمات السحابية بسبب مرونتها وقابليتها للتوسع، لكن هذا الاعتماد يعرضها لتهديدات سيبرانية خطيرة[2]. ومن بين أنواع الهجمات الأنظمة السحابية هي:

- سرقة الهوية والوصول غير المصرح به:

تحدث هذه الهجمات عندما يتمكن المهاجمون من سرقة بيانات تسجيل الدخول للمستخدمين أو المسؤولين. بمجرد الوصول، يمكنهم نسخ البيانات، تعديلها، أو حتى حذفها.

- هجمات البرامج الضارة (Malware):

يتم تحميل برامج ضارة على الأنظمة السحابية، مما قد يؤدي إلى تعطيل الخدمات أو سرقة البيانات الحساسة.

- التنصت على البيانات (Eavesdropping):

إذا لم تكن البيانات المرسلة بين المكتبة والمستخدمين مشفرة بشكل كافٍ، يمكن للمهاجمين اعتراضها وقراءة محتواها[3].

- هجمات رفض الخدمة (DDoS):

يركز هذا الهجوم على تعطيل الخدمة في الشبكة، حيث يقوم المهاجمون بإرسال كميات كبيرة من البيانات عبر الشبكة (أي إجراء الكثير من طلبات الاتصال)، هذا الهجوم لا يتم من خلاله سرقة للمعلومات ولا يمثل أي خرق أمني وانما يجعل المواقع الالكترونية وخدماتها عبر الانترنيت غير قابلة للوصول مما قد يسبب خسارة كبيرة للمؤسسة.

- الثغرات البرمجية واستغلالها:

---

[1] . رملي، فهمي؛ وزواوي، لمياء. **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**. المجلة الجزائرية للأمن والتنمية. المجلد، 12. العدد، 02، 2023. ص151

[2] . رملي، فهمي؛ وزواوي، لمياء. **المرجع السابق**. ص153

[3] . إبراهيم أحمد، علياء. **دور الحوسبة السحابية في تطوير خدمات المعلومات في المكتبة الجامعية: دراسة حالة على المكتبة المركزية بجامعة الإمام عبد الرحمن بن فيصل**. مجلة الدراسات الجامعية للبحوث الشاملة. المجلد، 05. العدد، 33، 2024. ص 14769

يمكن أن تستغل الثغرات الأمنية في التطبيقات أو الأنظمة السحابية للوصول غير المصرح به أو تنفيذ هجمات أخرى.[1]

3.2.3مخاطر وتهديدات تكنولوجيا الذكاء الإصطناعي:

تسعى المكتبات اليوم إلى دمج تقنيات الذكاء الاصطناعي لتحسين خدماتها وتلبية احتياجات المستخدمين في العصر الرقمي. ومع ذلك، فإن هذا التحول التكنولوجي يرافقه العديد من المخاطر التي تؤثر على الوظائف الأساسية للمكتبات، وهي توفير المعرفة وحفظها وإتاحتها للجميع. يمكن تفصيل هذه المخاطر كما يلي:[2]

أ. التحيز الخوارزمي والمعلوماتي:

أنظمة الذكاء الاصطناعي تعتمد على الخوارزميات والبيانات المدخلة لتوفير توصيات ونتائج بحث مخصصة. إذا كانت هذه البيانات تعكس تحيزات معينة، مثل التركيز على ثقافات أو لغات دون غيرها، فقد يؤدي ذلك إلى تعزيز هذا التحيز. على سبيل المثال، قد يتسبب التحيز في تهميش المحتوى الثقافي أو الأدبي المحلي لصالح مواد أكثر انتشارًا عالميًا، مما يُضعف التعددية الثقافية التي تسعى المكتبات لدعمها.

ب. انتهاك الخصوصية:

المكتبات تستخدم الذكاء الاصطناعي لتحليل سلوكيات المستخدمين بهدف تحسين التوصيات وخدمات البحث. يمكن أن يؤدي هذا إلى جمع بيانات شخصية حساسة، مثل عادات القراءة والبحث، مما يثير مخاوف بشأن كيفية تخزين هذه البيانات ومن يمكنه الوصول إليها. في حال اختراق النظام أو إساءة استخدام البيانات، فإن سمعة المكتبة ومصداقيتها قد تتعرضان للخطر.

ج. تحديات أمنية:

يمكن أن يُستغل الذكاء الاصطناعي في هجمات سيبرانية متقدمة تستهدف أنظمة المكتبة الرقمية. على سبيل المثال، قد يتم التلاعب بالخوارزميات لتغيير محتوى المكتبة الرقمي أو تعطيل الوصول إلى مواردها.[3]

---

[1] . إبراهيم أحمد، علياء. **المرجع نفسه**. ص 14769

[2]. السيد أحمد علي. منال. **تطبيقات تقنيات الذكاء الاصطناعي بالمكتبات الجامعية**. مجلة العربية الدولية. المجلد، 03. العدد، 03، 2023. ص 74 - 75

[3] . هندي عبد الله، أحمد. **استخدام الذكاء الاصطناعي في مجال المكتبات والمعلومات دراسة ببليومترية**. مجلة العلوم الإنسانية والاجتماعية. المجلد، 02. العدد، 03، 2022. ص 126

د. **فقدان المهارات البشرية:**

مع الاعتماد المتزايد على الذكاء الاصطناعي، قد تصبح بعض المهام التي يقوم بها أمناء المكتبات مؤتمتة بالكامل. ورغم أن هذا يُحسن الكفاءة، فإنه قد يؤدي إلى تقليص دور الإنسان في تقديم الخبرة والتوجيه الشخصي، مما يُضعف العلاقة التقليدية بين المستخدمين وأمناء المكتبات.[1]

4.2.3مخاطر وتهديدات تكنولوجيا أنترنت الأشياء

مع التطور التكنولوجي السريع، أصبحت المكتبات الجامعية تعتمد بشكل متزايد على التقنيات الحديثة لتعزيز خدماتها وتحقيق كفاءة عالية في تلبية احتياجات الباحثين والطلاب. إنترنت الأشياء (IoT) يُعد واحدًا من أبرز هذه التقنيات، حيث يسمح بربط الأجهزة والأنظمة المختلفة داخل المكتبة من خلال الشبكة، مما يسهم في تحسين إدارة الموارد، تسهيل الوصول إلى المحتوى، وتعزيز تجربة المستخدم. ومع ذلك، فإن هذا الاعتماد المتزايد على إنترنت الأشياء يحمل معه تحديات كبيرة تتعلق بالأمن السيبراني. تُعد المكتبات الجامعية، بما تحتويه من قواعد بيانات غنية وموارد معلوماتية حساسة، أهدافًا جذابة للهجمات السيبرانية. تشمل هذه التهديدات محاولات اختراق البيانات، الوصول غير المصرح به إلى الأجهزة المتصلة، وتعطيل الأنظمة التي تعتمد عليها المكتبات.[2] هذه التهديدات لا تؤثر فقط على كفاءة المكتبات في تقديم خدماتها، بل قد تُعرّض خصوصية المستخدمين وأمان معلوماتهم للخطر. لذلك، أصبح من الضروري تسليط الضوء على هذه التحديات ودراسة سبل التصدي لها لضمان استمرارية المكتبات الجامعية في تقديم خدماتها بأمان وفعالية في ظل تطور التقنيات الرقمية. ويمكن اختصار هذه التهديدات فيما يلي:

أ. **الثغرات الأمنية والهجمات السيبرانية:**

تعتمد المكتبات التي تتبنى إنترنت الأشياء على أجهزة متصلة بالشبكة، مثل الأرفف الذكية التي تُحدث بيانات المخزون تلقائيًا، وأجهزة الإعارة الذاتية، وحساسات تتبع الحضور أو التحكم في المناخ. إذا لم تكن هذه الأجهزة مؤمنة بشكل كافٍ، فإنها تُشكل نقاط ضعف يمكن للقراصنة استغلالها للوصول إلى بيانات المستخدمين، تعطيل الخدمات، أو حتى سرقة الكتب والمحتوى الرقمي.

---

[1] . السيد أحمد علي. منال. **المرجع السابق**. ص 75

[2] . نيل،خيرة ؛صادوق، خضرة. **تطبيقات انترنيت الأشياء في المكتبات: دراسة نظرية**. مجلة الرواق للدراسات الاجتماعية والإنسانية. المجلد، 08. العدد، 02، 2022. ص 98 -99

ب. الخصوصية المهددة:

تجمع أجهزة إنترنت الأشياء بيانات هائلة، مثل أوقات دخول المستخدمين وخروجهم، واستخدامهم للخدمات داخل المكتبة. قد يؤدي هذا إلى شعور المستخدمين بالرقابة وانعدام الخصوصية، وهو أمر يتعارض مع الدور التقليدي للمكتبة كمساحة حرة للتعلم والاكتشاف[1].

ج. التحديات التشغيلية:

في حال تعطل أنظمة إنترنت الأشياء، قد تُصاب المكتبة بشلل وظيفي. على سبيل المثال، إذا توقف نظام الإعارة الذاتية أو فشل جهاز تحديد المواقع الذكية للكتب، فإن ذلك يعيق عمليات المكتبة ويؤثر سلبًا على تجربة المستخدمين.

د. زيادة التكاليف البيئية:

أجهزة إنترنت الأشياء تحتاج إلى طاقة مستمرة للعمل، مما يزيد من استهلاك الطاقة. كما أن دورة حياة هذه الأجهزة قصيرة نسبيًا، ما يعني زيادة النفايات الإلكترونية التي تحتاج إلى إدارة سليمة، وهي تحديات تتعارض مع التزامات المكتبات بالاستدامة البيئية.[2]

5.2.3المخاطر والتهديدات الداخلية والخارجية في المكتبات الجامعية :

1.5.2.3المخاطر والتهديدات الداخلية:

وتشمل في المقام الأول الخروقات العرضية الحاصلة من قبل الموظفين بسبب الإهمال أو غير المطابقة وسوء سلوك الموظف العامل على الأنظمة. ويمكن الإشارة الى خارطة التهديدات الداخلية المحتملة، وتحتوي على أربعة عناصر وهي اختراق بيانات الشبكة، الاستخدام غير الفعال للأجهزة، ضعف التعليم، سرقة أجهزة الحاسب المحمول. وهذا النوع من التهديدات يخص التهديدات البشرية والتي بأنها أحداث تتم عن طريق أخطاء البشر، مثل أعمال غير مقصودة (ادخال بيانات غير مقصودة) أو إجراءات متعمدة مثل: (الهجوم على الشبكة، تحميل البرمجيات الخبيثة، الوصول الغير مصرح به الى المعلومات السرية[3]).

---

[1] . مقراني، قدور؛ عطايت الله، ربيع. **التحديات الأمنية لأنترنيت الأشياء**. المجلة الجزائرية للدراسات الاقتصادية والإدارية. المجلد، 01. العدد، 02، 2021. ص 64 – 66

[2] . هندي عبد الله، هندي أحمد. **المرجع السابق**. ص 130

[3] . الطائي، محمدعبد الحسين؛ الكيلاني،محمود. **المرجع السابق**. ص119

ويمكن تصنيف التهديدات البشرية الى نوعين رئيسيين:

- العاملون:

أي أن المسبب التهديدات الأمنية هو الخطأ البشري، يكون المعنى بذلك هم الموظفون والعاملون في المكتبة، اذ يشكل الموظفون ما نسبته 80 بالمئة من مصادر التهديدات الداخلية في المكتبة وتشمل هذه الفئة الموظفين الحاليين والسابقين، والمهاجمون من الداخل هم "أولئك الافراد الذي ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية الى حماية أنظمة المعلومات التي تستخدمها تلك الجهة."[1]

التهديد من الداخل يمكن ان يكون حدث ضار مقصود وغير مقصود، عن أشخاص متعمدين، للوصول الى نظم المعلومات داخل المكتبة في الشبكة. والعاملون من الداخل كانوا دوما الخطر الذي تواجهه أي جهة. مهما كانت سواء كانت تلك الجهة شركة أو منظمة. ومع استخدام الحاسوب والتقنيات زاد الخطر الناجم عن الهجمات التي تقوم بها العاملون من الداخل ضد الجهة التي ينتمي اليها. ويؤكد المتخصصون أن الهجوم من الداخل لا يحصل دون أسباب حقيقية. حيث أن هناك أسباب مختلفة للهجوم ضد نظم المعلومات، وهذه الأسباب يمكن ايجازها كالآتي:

- حالة عدم الرضا على العمل ومن ثم يقوم بمهاجمة نظم المعلومات للانتقام.
- اثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم اليكتروني، حيث هناك بعض الأفراد يشعرون بالفخر والاعتزاز بنفسهم.
- تحقيق مكاسب مالية، حيث يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات سرية يستخدمها للابتزاز الجهة لدفع فدية مالية[2].

هناك العديد من تلك الأخطاء التي تشكل تهديدا كبيرا على امن المعلومات في المكتبة، وتشكل الأخطاء التقنية من بين أسوء الأخطاء التي يرتكبها المستخدمون لأنظمة المعلومات ومنها:

- عدم الاحتفاظ بنسخ احتياطية واختبارها.
- عدم القيام بتحديث الأنظمة عند اكتشاف فجوات امنية فيها.
- ربط الأنظمة بالأنترنيت قبل تشغيل أنظمة الحماية.

[1] . الطائي، محمدعبد الحسين؛ الكيلاني،محمود. **المرجع نفسه**. ص 120

[2] . الطائي، محمدعبد الحسين؛ الكيلاني،محمود. **المرجع السابق**. ص 122

- الاستهانة بالمخلفات التقنية أمر بالغ الخطورة، اذ يقوم المهاجم بتفتيش المخلفات التقنية الخاصة بالمكتبة الموجودة في القمامة والمواد المتروكة كمخلفات بحثا عن أي شيء يساعده على اختراق النظام، مثل الأقراص الصلبة بعد استبدالها، أو الأوراق التي دون عليها كلمات السر أو أسماء الملفات والبرامج[1].

المهاجمون: وهم الأشخاص من خارج المكتبة والذين يطلق عليهم "القراصنة Hacker" والذين لديهم بواعث مختلفة للهجوم على الأنظمة، وهم أكثر خطورة من الموظفين الساخطين.[2]

القراصنة: القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول للنظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطوري الأنظمة في النظام. وبالإضافة الى ذلك، العديد من المتسللين بارعون في اكتشاف كلمات السر للمستخدمين المرخص لهم الذي يفشلون في اختيار كلمات المرور التي يصعب تخمينها أو تلك غير المدرجة في القاموس. تمثل أنشطة القراصنة تهديدات خطيرة للمعلومات السرية في أنظمة الحاسوب. حيث أنشأ العديد من المتسللين نسخ من الملفات ذات الحماية غير الكافية وتم وضعها في مجالات النظام والتي يمكن الوصول اليها من قبل الأشخاص غير مخولين.[3]

2.5.2.3المخاطر والتهديدات الخارجية:

هذا النوع من المخاطر يكون مصدره أسباب من الخارج النظام أي يمكن أن يكون نتيجة أشخاص مخولون باستخدام النظام أو من أسباب طبيعية وبيئية ومن هذه المخاطر ما يلي:

- الهجوم الأمني: الهجوم الأمني يشير إلى محاولات غير مشروعة تهدف إلى الوصول إلى الأنظمة أو البيانات المحمية داخل المكتبة. يمكن أن تشمل هذه الهجمات البرمجيات الخبيثة مثل الفيروسات، أو استغلال نقاط الضعف في الشبكة لإتلاف الأنظمة، أو تعطيل الخدمات الإلكترونية التي تقدمها المكتبة، مما يؤثر على تقديم المعلومات والخدمات للمستفيدين.
- خطر الاختراق: خطر الاختراق يشير إلى محاولات قراصنة الإنترنت للوصول غير المصرح به إلى بيانات المكتبة أو أنظمتها. قد يستهدف المخترقون قواعد البيانات التي تحتوي على معلومات حساسة، مثل بيانات المستخدمين أو المواد النادرة، مما يهدد أمن وخصوصية المكتبة ومرتاديها[4].

---

[1] . بوخنفر، زوليخة. **المرجع السابق**. ص 80

[2]. خنوسي، كريمة. **الحماية الدولية من جرائم التقليد والقرصنة الإلكترونية وموقف المشرع الجزائري منها**. مجلة مصداقية. المجلد، 03. العدد، 03، 2021. ص 59

3. خنوسي، كريمة.**المرجع السابق**، ص61-63

[4] . حسين، عميروش؛ بلعسل بنت نبي، ياسمين.**التهديدات الالكترونية للأمن السيبراني في الوطن العربي**. مجلة نوميروس الأكاديمية. المجلد، 02. العدد، 02، 2021. ص 175 – 177

- الاصطياد الإلكتروني: الاصطياد الإلكتروني هو نوع من الاحتيال الذي يعتمد على استهداف المستخدمين عبر البريد الإلكتروني أو الرسائل الوهمية لإقناعهم بالكشف عن معلومات حساسة، مثل كلمات المرور أو بيانات الحساب. يشكل هذا تهديداً كبيراً للمكتبات إذا تعرض الموظفون أو المستخدمون لمثل هذه الحيل، ما قد يؤدي إلى اختراق الأنظمة أو سرقة البيانات.
- المخاطر الطبيعية والبيئية: المخاطر الطبيعية والبيئية تشمل الكوارث الطبيعية مثل الزلازل، الفيضانات، الحرائق، أو الأعاصير التي قد تلحق أضراراً جسيمة بالبنية التحتية للمكتبة ومحتوياتها من الكتب والمخطوطات والمعدات. إضافة إلى ذلك، التغيرات البيئية كالرطوبة العالية قد تؤدي إلى تلف المواد الورقية والأرشيفية إذا لم تتخذ تدابير الحماية المناسبة.[1]

3.3 إستراتجية إدارة مخاطر الأمن السيبيراني في المكتبات الجامعية

التطور الذي يلاحق المكتبات الجامعية لم يأت وليد الصدفة بل يدخل في كنف التطورات التي تجري على نطاق واسع نتيجة التكنولوجيات الحديثة التي أصبحت جزء لا يتجزأ من العملية التسييرية للمكتبات، إلا أنها وجدت نفسها في مواجهة العديد من المخاطر والأزمات، التي قد تتعرض لها في أي لحظة وما أن تجد نفسها قد استكملت الإجراءات الخاصة بالوقاية من خطر معين إلا وتجد خطر جديد يهدد كيان ووجود هذه المؤسسة سواء كان ماديا أو معنويا.[2] هذا ما أدى إلى ضرورة وضع إستراتيجيات من أجل إدارة مخاطر الأمن السيبيراني في المكتبات الجامعية، وهي مجموعة من الخطط والسياسات والإجراءات المصممة لحماية المعلومات والأنظمة الرقمية من التهديدات السيبرانية والهجمات الإلكترونية هدفها الرئيسي ضمان سرية البيانات وسلامتها وتسهيل إمكانية الوصول إليها بشكل آمن ومواجهة التهديدات والمخاطر بفعالية[3].

ولقد أظهرت التجربة السعودية نجاح كبير في بناء الإستراتيجية الوطنية للأمن السيبراني ممثلة في الهيئة الوطنية للأمن السيبراني، تعمل الهيئة على تحقيق ستة أهداف رئيسية لتأسيس منظومة متكاملة وهي كالآتي:

1. حوكمة متكاملة للأمن السيبراني على مستوى المملكة.
2. حماية الفضاء السيبراني.
3. تعزيز الشراكات والتعاون في الأمن السيبراني.
4. إدارة فعالة للمخاطر السيبرانية على المستوى الوطني.

---

[1] . الكيلاني، ينال محمود. وعبد الحسين الطائي، محمد. **المرجع السابق**. ص 125

[2] . بن عديد، سامية.**مخاطر الامن السيبراني والمعلوماتي وتطور المعرفة التقنية على برامج الحماية للأنظمة المعلوماتية**.كتاب جماعي: الأمن المعلوماتي ورقمنة قطاع التعليم: جامعة سوق أهراس، 2023.ص 34

[3]. بارشيد، ناهد عبد الله؛ عبيد راوية رضا. **أثر الإستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية: دراسة ميدانية على القطاعات الحكومية السعودية**. مجلة إدارة المخاطر والأزمات، المجلد،06، 2025.ص05

5. تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية.
6. بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني[1].

تتضمن إعداد الإستراتيجية لإدارة مخاطر الأمن السيبراني والتقليل من التهديدات مجموعة من الإجراءات وهي كالآتي:

- تحليل البيئة الداخلية والخارجية للمؤسسة.
- تحديدالمخاطر المحتملة.
- تصميم إجراءات الأمن السيبراني وتنفيذها وأيضا تطوير التكنولوجيا السيبرانية.
- تدريب الموظفين في مجال التقنية والأمن السيبراني.
- تقييم الأمان بشكل دوري[2].

من جهة أخرى، أظهرت بعض الدراسات أن صياغة وبناء إستراتيجية تضمن حماية المعلومات وخصوصية وسرية البيانات يشترط توفر ضوابط وهي كالآتي:

1.تطبيق معايير الأمان الدولية:

تلعب معايير الأمان الدولية دورًا حيويًا في إدارة مخاطر الأمن السيبراني داخل المكتبات الجامعية، حيث تمثل هذه المعايير إطارًا موحدًا يضمنحماية البيانات والمعلومات الحساسة من التهديدات الرقمية المتزايدة. ومن بين هذه المعايير، تأتي ISO/IEC 27001 التي توفر إرشادات لإنشاء نظام إدارة أمن المعلومات (ISMS)، مما يعزز قدرة المكتبات على التعرف على المخاطر ومعالجتها بشكل استباقي. تطبيق هذه المعايير يساعد في تأمين قواعد البيانات، وحماية معلومات المستخدمين، وضمان استمرارية الخدمة. كما يعزز التزام المكتبات الجامعية بهذه المعايير الثقة بين الطلاب وأعضاء هيئة التدريس، حيث يطمئنهم بأن بياناتهم الأكاديمية والشخصية محمية وفقًا لأفضل الممارسات العالمية.[3]

---

[1]. الهيئة الوطنية للأمن السيبراني. تارخ الإطلاع(10-01-2026)، متاح عل الرابط:https://nca.gov.sa/

[2]. بارشيد، ناهد عبد الله؛ عبيد راوية رضا. **المرجع السابق**.ص05

[3]. كادي، زين الدين؛ غوار، عفيف. **إدارة الجودة الشاملة ومعايير الايزو في المكتبات الجامعية الجزائرية: دراسة ميدانية بالغرب الجزائري**. مجلة الحضارة الإسلامية. المجلد، 05. العدد، 04، 2014. ص 248

أ.معيار ISO/IEC 27001:

هو معيار دولي يُحدد متطلبات إنشاء وتشغيل وصيانة وتحسين نظام إدارة أمن المعلوماتISMS، يهدف هذا المعيار إلى مساعدة المؤسسات على حماية أصولها الرقمية والمعلوماتية من التهديدات السيبرانية وضمان سرية المعلومات وسلامتها وتوافرها. ومن أهم مبادئ هذا المعيار[1] ما يلي:

- إدارة المخاطر: يُركز المعيار على تقييم المخاطر الأمنية المرتبطة بالمعلومات وإدارتها بشكل فعال.
- السياسات والإجراءات: يضع إطارًا لتطوير سياسات وإجراءات أمنية تُحدد كيفية التعامل مع البيانات والأنظمة.
- التحسين المستمر: يدعو إلى مراجعة دورية للأنظمة الأمنية وتحسينها بناءً على التغيرات في التهديدات أو احتياجات المؤسسة.
- التوافق مع القوانين: يساعد المؤسسات على الالتزام بالتشريعات المحلية والدولية المتعلقة بحماية البيانات.
- التدقيق الداخلي: يُشجع على إجراء مراجعات داخلية منتظمة لضمان الامتثال للمعايير[2].

ومن أهم فوائد تطبيق هذا المعيار خاصة كأداة لتحسين مستوى الأمان السيبيراني خاصة في المكتبات الجامعية ما يلي:

- حماية البيانات الحساسة.
- تعزيز ثقة العملاء والمستخدمين.
- دعم المؤسسات في الحصول على اعتماد دولي يبرز التزامها بالأمان السيبراني.
- يُعد هذا المعيار أداة قوية لأي مؤسسة، بما في ذلك المكتبات الجامعية، لحماية بياناتها وتوفير بيئة معلوماتية آمنة.

ب.معيار ISO:

وضع معايير لمصادر المعلومات في البيئة الرقمية هدفه الأساسي حماية الملكية الفكرية من السرقات العلمية وحفظ براءة الاختراعات لكل شخص بغض النظر عن اهداف أخرى مثل وصول الحر واتاحة المعلومات وجودة الخدمات في المكتبات الجامعية او مراكز المعلومات بصفة عامة، بعد التعرف على مفهوم البيئة الرقمية وخصائصها لبد من معرفة مفهوم الملكية الفكرية عامة وفي البيئة الرقمية خاصة. تولي المنظمة العالمية لتقييس ايزو أهمية كبيرة لأمن المعلومات نظرا لتوسع استعمال تقنيات المعلومات وكثرة التهديدات سواء للمنظمات او للأفراد، ومن بين اهم

---

1. Iso/IEC27001: 2022.**Information Security. Cyber Security and privacy protection information security management systems requirements**. Https:// www.iso / standard/27001 .19:23h

2. Iso/IEC27001: 2022.**Op.Cit**

معايير تكنولوجيا المعلومات نجد عائلة المعيار ISO/ IEC، JTC1/ SC27، وهما امن المعلومات والأمن السيبراني وحماية الخصوصية، حيث تضم جملة من البنود والتوجيهات من بينها وأهمها نجد إدارة الهويات وخاصة في بيئة رقمية لبد من تحديدها ثم منهجية إدارة المعلومات وأمن تكنولوجيا المعلومات والاتصالات، آليات التشفير وسرية المعلومات، معرفة المكونات الأمنية للمعلومات كما تضمنت معايير منهجية تقييم فعالية آمن المعلومات، وأصدرت معايير أخرى من بينها عائلة " IEC/ IS 27000" التي تهتم بتقنيات آمن المعلومات ونظم تسيير آمن المعلومات في ظل تكنولوجيا المعلومات[1].

2.وضع سياسات الأمان والإجراءات الداخلية:

أ. الممارسات الجيدة:

بالإضافة إلى التكنولوجيا فالحس السليم والحذر الدائم يسمحا لنا في الكثير من الأحيان تجنب مخاطر الفضاء السيبراني. في هذا الإطار نعرض بعض الممارسات الجيدة التي يجب على مستعمل الفضاء السيبراني أخذها بعين الاعتبار:

- السيطرة على ردود أفعالنا العاطفية الأمن السيبراني للعقل البشري.
- كن حذرا مع هاتفك الذكي أو جهازك اللوحي.
- كن حذرا عند استخدام نظام المراسلة الخاص بك.
- كلمات المرور يجب أن تكون معقدة وقوية وأن تغيَّر بانتظام، ولكل تطبيق كلمة مرور خاصة به.
- أن تكون لديك إستراتيجية حفظ البيانات منتظمة ومخطط لها بشكل صحيح ودقيق.
- فصل الاستخدامات الشخصية عن الاستخدامات المهنية.
- عدم تثبيت برامج أو تطبيقات من مواقع غير رسمية.
- عند نهاية استعمال البريد الاليكتروني أو تصفح الأنترنيت باستعمال الحاسوب يستحسن إيقاف تشغيلها حتى لا تستطيع مجرم سيبراني قرصنتها أو استغلالها لأغراض دنيئة[2].

3.تحديد سياسة التأمين التشغيلي:

يعد وجود خطة استراتيجية لتعزيز الأمان الرقمي بالمكتبة من الأمور الهامة؛ حيث أنها تعمل على زيادة وسرعة توجه المكتبة نحو تحقيق أهدافها المرجوة والحفاظ على نشاطها، فمن خلال تلك الخطة الاستراتيجية يمكن للمكتبة تحديد أولوياتها من التأمين التشغيلي والتركيز عليها، وكذلك تحديد أوجه القصور والعمل على تحسينها؛ ومن ثم

---

[1]. **Iso/IEC27001: 2022**. Ibid

[2] . بوقرص، ساعد. **المرجع السابق**. ص 79

تفادي المخاطر الرقمية التي قد تواجه الأجهزة والشبكات بالمكتبة، إلا أنه تبين من خلال الجزء التطبيقي للبحث عدم وجود خطة استراتيجية لتعزيز الأمان الرقمي أجهزة الحاسب الآلي وحمايتها من المخاطر الرقمية مما يزيد من احتمالية تعرض أجهزة الحاسب الآلي بالمكتبة للمخاطر الرقمية يوما ما.[1]

4.سياسة الاعدادات والتحصين:

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية وتحصين وضبط إعدادات الأصول المعلوماتية والتقنية والتطبيقات الخاصة بالمكتبات الجامعية ومقاومة الهجومات السيبرانية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسالمتها، وتوافرها.[2]

5.الإمتثال للقوانين والتشريعات المحلية والدولية للأمن السيبراني:

مع بداية القرن الواحد والعشرين استطاعت الثورة الرقمية احداث حراك معرفي واسع، في ادراك أنماط تفاعلات الفضاء الرقمي، فأصبح حجم وتأثير الدول ومكانتها معرفا بقدراتها في امتلاك وتوطين وسائل التكنولوجيا وتم إعادة قراءة مفاهيم القوة والسيادة تماشيا مع أشكال التهديد الجديد للأمن الدول، انطلاقا من حروب الجيل الرابع والخامس المنبعثة من استغلال الفضاء السيبيراني، عن طريق شن هجمات اليكترونية وتنفيذ جرائم سيبرانية تستهدف المساس بأمن المؤسسات والدول وحتة الأشخاص مما أصبح يفرض استجابة أمنية وقانونية، والجزائر أحد أكبر الدول تعرضا للهجمات السيبرانية بشقيها الاجرامي والأمني مما دفعها ال جعل قضايا الأمن السيبراني في عمق الشواغل الأساسية والمستجدة لبرامج السياسات الأمنية والاستراتيجية، خاصة في ظل الجهد المتسارع للجزائر نحو تبني التحول الرقمي لحوكمة الأنشطة والقطاعات، وتماشيا مع هذه المعطيات الجديدة انبرت حقول الدراسات الأمنية والتشريعية لاستيعاب هذه الحركيات الجديدة ضمن مصفوفات حماية الأمن الشامل. واتجهت الدول لصيانة أمنها السيبيراني عبر استراتيجيات دفاعية وحمائية سعيا منها للتصدي لمختلف مخاطر الأمن السيبراني.[3]

ويتم قياس هذه الاستراتيجية من خلال النموذج الذي أعلنه الاتحاد الدولي للاتصال ITU حيث وضع نموذج من أجل بناء استراتيجية الوطنية للأمن السيبراني، ويتضمن هذا النموذج عدة محاور أساسية: الأول يرتبط بالتدابير القانونية والتشريعية، والثاني يتعلق بالتدابير التقنية، والمحور الثالث خاص بالهياكل التنظيمية المؤسسية

---

[1] . علي شتا عبد السلام، ابتسام. **المرجع السابق**. ص 42

[2] . علي شتا عبد السلام، ابتسام. **المرجع السابق**. ص 44

[3]. محمودي، سعيد. **الأمن السيبراني في الجزائر: بين المعالجة الأمنية والحماية القانونية**. مجلة الناقد للدراسات السياسية. المجلد، 07. العدد، 02، 2023. ص 194- 195

للأمن السيبيراني في الدولة، والمحور الرابع مرتبط ببناء القدرات الفنية في هذا المجال الذي يعاني ندرة المتخصصين، وأخيرا يتناول المحور الخامس التعاون الدولي وتبادل المعلومات بين الدول في مجال الأمن السيبيراني. [1]

وتتمثل هذه القوانين والتشريعات فيما يلي:

أ.المنظومة القانونية:

في إطار مراجعة قوانين الجمهورية لتكييفها مع التطورات التكنولوجية العالمية وأيضا مع المعاهدات والاتفاقيات الدولية التي أبرمتها الجزائر من أجل مواكبة عصر المعلومات راجعت الجزائر القوانين التالية:

- قانون رقم 15/04 سنة 2004 المتضمن تعديل قانون العقوبات وقد أدرج في قسمه السابع مكرر موضوع المساس بأنظمة المعالجة الالية للمعطيات من خلال إقرار العقوبات المتعلقة بأي سلوك أو تصرف من شأنه المساس أو الاضرار بالمعطيات والهيئات والمؤسسات المنصوص عليها في المادة 394.
- قانون رقم 04/09 سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها حيث هدف هذا القانون ال وضع القواعد الخاصة للوقاية من الجرائم كما وضع بعض المصطلحات المرتبطة بتكنولوجيا الاعلام والاتصالات مثل: التعريف بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال، ومصطلحات منظومة معلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة سير أي معطيات متعلقة بالاتصال عن طريق المنظومة المعلوماتية، والاتصالات الالكترونية كما حدد هذا القانون الحالات التي يسمح بها باللجوء ال المراقبة الالكترونية في المادة 04 [2]كما يلي:
  - ✓ الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة.
  - ✓ في حالة توفر معلومات احتمال اعتداء عل المنظومة المعلوماتية عل نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الرقمي.
  - ✓ لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول ال نتيجة تهم الأبحاث الجارية دون اللجوء ال المراقبة الالكترونية.
  - ✓ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

[1] . محمودي، سعيد. **المرجع نفسه**. ص 197

[2].بن خضير، أحمد بن عبد الله. **المرجع السابق**.ص145-146

✓ كما يحدد هذا القانون ان المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات المؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[1].

- قانون 03/15 سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، حيث حددت مادة 05 فيه انه يجب ان تتواجد عل التراب الوطني كل البيانات والمعلومات ذات الطابع الشخصي التي تم جمعها من مؤدي خدمات التصديق الالكتروني أو الطرف الثالث الموثوق أو السلطات التصديق الالكتروني وكذلك قواعد البيانات التي تحتويها ولا يمكن نقلها ال خارج التراب الوطني في الحالات التي ينص عليها التشريع المعمول به.

- قانون 04/18 سنة 2018 المحدد للقواعد العامة بالبريد والاتصالات الالكترونية حيث وضع أن نشاطات البريد والاتصالات الالكترونية تخضع لرقابة الدولة، وأن هذه الأخيرة تمارس صلاحيتها وفق ما يلي:

  - ممارسة السيادة طبقا للأحكام الدستورية عل كامل فضائها الهيرتيزي.
  - الانفراد بالاستعمال الحصري لطيف الذبذبات اللاسلكية وضمان التخطيط وتقسيمه ال ذبذبات ومراقبته والاشراف عل استعماله من طرف المستعملين في ظل احترام مبادئ الفعالة والرشادة في استعمال الذبذبات اللاسلكية الكهربائية.
  - تحديد قواعد شغل الأملاك العمومية والاستفادة من الارتفاعات المرتبطة بانتشار الاتصالات الالكترونية وباستعمال الفضاء الهيرتيزي.
  - السهر على تطبيق اتفاقات وأنظمة وتوصيات الاتحاد الدولي للاتصالات[2].

كما قدم هذا القانون تعريفا للأمن السيبيراني بأنه: "مجموع الأدوات والسياسات ومفاهيم الأمن والأليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإليكترونية ضد أي حدث من شأنه المساس يتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة [3]".

- قانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في ذات السنة، وقد تضمن هذا القانون تفصيلا للمقصود بهذه المعطيات واليات المعالجة والمبادئ الأساسية

---

[1]. بن خضير، أحمد بن عبد الله. **المرجع نفسه**.146

[2]. الجريدة الرسمية الجزائرية. المرسوم التنفيذي رقم 04/18 المؤرخ في 24 شعبان عام 1934 الموافق ل10 ماي سنة 2018 يتضمن القواعد العامة التعلقة بالبريد والإتصالات الرقمية، العدد 27، 2018.ص04-05

[3]. المادة 10 من القانون 04/18.**المرجع السابق**.ص.07

لحماية المعطيات ذات الطابع الشخصي في إطار حفظ الكرامة الإنسانية وعدم المساس بها وحماية الحياة الشخصية والحريات العامة وألا مس بحقوق الأشخاص وشرفهم وسمعتهم. محددا مصطلح معالجة المعطيات ذات الطابع الشخصي عل أنه "كل عملية أو مجوعة عمليات منجزة بطرق أو برسائل الية أو بدونها عل معطيات ذات طابع شخصي مثل جمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الايصال عن طريق الارسال أو النشر أو أي شكل من اخر الاشكال الاتاحة أو التقريب أو الربط البيئي وكذا الاغلاق والتشفير أو المسح أو الاتلاف"، كما أكد المشرع الجزائري عل حماية المعطيات ذات الطابع الشخصي للأطفال باعتبارهم شريحة عامة من المجتمع وأيضا كأفراد لهم حماية خصوصية. حيث جاء في النص المادة 08 " لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بالطفل الا بعد الحصول عل موافقة ممثله الشرعي أو عند الاقتضاء بالترخيص من القاضي المختص.

- أيضا صدر قانون 02/18 سنة 2018 المتعلق بالتجارة الالكترونية حدد هذا القانون القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات، كما حدد المستهلك الالكتروني، المورد الالكتروني، الاشهار الاليكتروني وكذا وسيلة الدفع الالكترونية، وكذا الجرائم والعقوبات المترتبة عنها. وبناءا على هذا نجد الجزائر ركزت بشكل أساسي على الجرائم السيبرانية بداية من صدور قانون العقوبات 2004 الى قانون 2009 ثم سنة 2015 أصدرت قانون التوقيع والتصديق الالكتروني الذي لا يزال يعرف تأخرملحوظا في التطبيق أيض أصدرت قانون حماية المعطيات الشخصية وقانون البريد والاتصالات الالكترونية، ثم قانون التجارة الالكترونية 2018 وهو ما يعكس توجهات الدولة الأمنية وأيضا يرجع لتخلف الجزائر في مجال الاقتصاد الرقمي والتجارة الالكترونية ووسائل الدفع الالكتروني وكذا تأخر البنوك المصرفية الجزائرية في تطبيق نظام العاملات الالكترونية واعتمادها على المعاملات التقليدية.

4.3.تقنيات وأدوات الأمن السيبيراني بالمكتبات الجامعية

1.4.3تدابير وقائية لمواجهة مخاطر الأمن السيبيراني:

مسألة أمن المعلومات في المكتبات الجامعية ضرورية جدا خاصة مع التهديدات التي تعاني منها من إشكالية السرقة كلمات المرور وتخريب قواعد البيانات أو أنظمة التشغيل والتجسس على بعض المعلومات الشخصية لمنتسبي هذه المكتبة هذا ما نتج عنه ضرورة وضع تدابير وقائية لمواجهة هذا النوع من المخاطر ومن بين هذه التدابير نذكر[1] منها:

[1] . كادي، زين الدين. **المرجع السابق**. ص 63

- أمن وحماية الولوج أو الدخول الى الأنظمة:

من وحماية الولوج أو الدخول إلى الأنظمة يشمل ضمان استخدام تقنيات متقدمة مثل كلمات المرور القوية، والمصادقة الثنائية، وتحديد صلاحيات المستخدمين بناءً على أدوارهم، مما يقلل من احتمالية الوصول غير المصرح بهن وذلك عن طريق تطبيق مجموعة من التدابير وهي كالآتي:

- يجب ألا تتضمن كلمة المرور معلومات شخصية.
- المزج بين الحروف والأرقام.
- تجنب تضمين اسم المستخدم داخل كلمة المرور.
- لا تحتفظ كلمة المرور في جهازك بدون تشفير.
- لا ستخدم خاصية الدخول التلقائي خاصة إذا كنت تستخدم جهازا عاما.
- كلمة المرور أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم، وفاعليتها تعتمد على درجة انضباط العنصر البشري في اختيار كلمة المرور والتعامل معها وفقلا الأساليب الصحيحة[1].

- أمن وحماية البرامج والتطبيقات:

أمن وحماية الولوج أو الدخول إلى الأنظمة يشمل ضمان استخدام تقنيات متقدمة مثل كلمات المرور القوية، والمصادقة الثنائية، وتحديد صلاحيات المستخدمين بناءً على أدوارهم، مما يقلل من احتمالية الوصول غير المصرح به. لاعتماد منهج الوقاية والسلامة من الفيروسات وأشباهها في المكتبات ومراكز المعلومات يجب اتخاذ التدابير التالية:

- لا تقم بفتح مرفق مع رسالة من شخص مجهول.
- لا تقم بفتح ملف مرفق برسالة من شخص معلوم الا إذا كنت تتوقع ذلك الملف.
- لا تقم بفتح وقراءة رسالة من أشخاص مجهولين تحمل عنوانا غريبا.
- قم بتعطيل ميزة تحميل الملفات المرفقة مع الرسالة الالكترونية.
- افحص أي ملف غريب عن طريق البريد الالكترونية أو المرسل الاتي.

[1] . كادي، زين الدين. **المرجع السابق**. ص 63

- افحص أي ملف تقم بتحميله وتأكد من خلوه من أي شبهة كانت.
- القيام بعمل نسخة احتياطية للملفات بشكل دوري في وحدة تخزين خارجية.
- استخدام برامج مكافحة الفيروسات وتحديثه بشكل دوري.
- عدم استخدام برامج مشاركة الملفات

- عقد تأمين الأخطار المعلوماتية:

عقد تأمين من الأخطار المعلوماتية يعتبر وسيلة وقائية مهمة لتغطية الخسائر الناتجة عن الهجمات الإلكترونية، حيث يوفر الحماية المالية للمكتبة في حال تعرضها للاختراق أو فقدان البيانات، مما يضمن استمرارية العمل بأقل تأثير ممكن، وبالتالي تامين في مجال المعلوماتية في مجال المكتبات الجامعية هو تامين هذا النظام كاملا ككل أو تامين سوف يقع فقط على كل ما يتعلق بالحواسيب وأجهزة الاعلام الالي، سواء في شقها المادي او على مستوى البرمجيات، وبما ان اجراءات التامين في هذه الحالة تتم بشكل عادي ككل إجراءات التأمين الأخرى العادية في حياتنا اليومية، ومع أي شركات التامين التي توفر هذه الفئة من عقود التامين. ومثال على ذلك:

- تأمين الأرصدة الوثائقية لما هناك من أخطار وكوراث طبيعية وبشرية تهددها.
- تأمين الأشخاص من عمال وموظفين.
- تأمين المباني ومحلات حفظ المعلومات[1].

- ضرورة تحقيق متطلبات الامن السيبيراني في المكتبات الجامعية:

التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.

ومن بين هذه المتطلبات لتحقيق الأمن المعلوماتي في البيئة المكتبية هي:

[1] . بن عديد، سامية.المرجع السابق.ص36-37

- يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني، وأن تكون متطلبات الأمن السيبراني جزء أساسي من متطلبات المشاريع التقنية.[1]

- يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة، وتقييم الثغرات ومعالجتها اجراء مراجعة لإعدادات والتحصين وحزم التحديثات قبل إطلاق وتدشين المشاريع والتغييرات.[2]

- يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى ما يلي: استخدام معايير التطوير الآمن للتطبيقات Standards Coding Secure.واستخدام مصادر مرخصة وموثوقة الأدوات تطوير التطبيقات والمكتبات الخاصة بها Libraires. بالإضافة الى اجراء اختبار للتحقق من مدى استيفاء التطبيقات للمتطلبات الأمنية السيبرانية للجهة أمن التكامل بين التطبيقات.[3]

2.4.3تقنيات الوقاية من مخاطر الأمن السيبيراني:

تعد المكتبات الجامعية من الركائز الأساسية لدعم البحث العلمي والتعليم الأكاديمي. ومع تزايد استخدام التكنولوجيا الرقمية لتخزين البيانات وإدارتها، أصبحت هذه المكتبات عرضة لمخاطر الأمن السيبراني مثل الاختراقات، الفيروسات، وسرقة البيانات. وللحد من هذه المخاطر، تعتمد المكتبات الجامعية على مجموعة من التقنيات الوقائية لضمان حماية بياناتها ومستخدميها. من بين أبرز هذه التقنيات: التشفير، النسخ الاحتياطي، وجدران الحماية.[4]

---

[1] . عبد الدايم أحمد الحداد، نبيلة. **متطلبات تحقيق الامن السيبيراني في المكتبات الجامعية اليمنية**. مجلة جامعة البيضاء. المجلد، 04. العدد، 02، 2022. ص 753

[2]. سمحان، منى عبد الله صال. **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**. مجلة كلية التربية بالمنصورة. المجلد، 01. العدد، 02، 2020. ص 29

[3] . عبد الدايم أحمد الحداد، نبيلة. **المرجع السابق**، ص 50

[4]. بلبكاي، جمال. **المكتبات الجامعية والتقنية**. مجلة الحكمة للدراسات الاجتماعية. المجلد، 04. العدد، 07، 2016. ص 125

1.2.4.3تقنية التشفير:

تقنية التشفير هي عبارة عن تقنية ادخال تعديلات على المعلومات عند ارسالها الى جهة معينة أو تحويلها الى رموز غير ذات معنى حيث عندما تصل الى اشخاص اخرون لا يستطيعون فهمها أو الاستفادة منها. لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة الى نصوص مشفرة وغير مفهومة وتبنى أساس أن كل معلومة تحتاج لفكها واعادتها الى الوضع الأصلي.

واستخدام تقنية التشفير في المكتبات الجامعية يتمثل في إعادة تحرير بيانات الكمبيوتر وتحويلها من نص مقروء إلى آخر غير مقروء من خلال خوارزميات خاصة؛ تجعل للمستخدم فقط سلطة التحكم في المعلومات، مما يعمل على تجنب سرقة المعلومات أو تسريبها أو تغييرها أو إتلافها بشكل غير قانوني[1]،

وتنقسم عملية التشفير إلى أنواع متعددة منها: تشفير الإرسال لحماية البيانات في عملية النقل، وتشفير التخزين لحماية البيانات في عملية التخزين وتشفير التكامل لحماية البيانات عن طريق التحقق من سلامة محتوى معالجة المعلومات ونقلها، واستخدام رمز التوقيع لتحقيق تأكيد التشفير.[2]

وتكمن أهمية التشفير من أبرز التقنيات الوقائية التي تعتمدها المكتبات الجامعية لحماية بياناتها وأنظمتها من التهديدات السيبرانية. يقوم التشفير بتحويل البيانات من شكلها المقروء إلى صيغة غير مفهومة باستخدام خوارزميات رياضية معقدة، بحيث لا يمكن فك تشفيرها إلا باستخدام مفتاح خاص. في المكتبات الجامعية، يُستخدم التشفير لتأمين قواعد البيانات التي تحتوي على معلومات حساسة مثل: بيانات الطلاب وأعضاء هيئة التدريس، سجلات استعارة الكتب، والاشتراكات في الموارد الرقمية. علاوة على ذلك، يُعزز التشفير أمان الاتصالات عبر الشبكات، مثل تبادل البيانات بين الخوادم والأجهزة أو الدخول إلى قواعد البيانات عن بُعد باستخدام بروتوكولات مثل HTTPS وSSL.[3]

وبالتالي هذه التقنية ليست فقط حاجزاً أمام المخترقين، بل تضمن أيضاً حماية البيانات حتى في حال وقوع اختراق، إذ تصبح المعلومات غير قابلة للقراءة أو الاستخدام. وبفضل هذا المستوى العالي من الأمان، يساعد التشفير المكتبات الجامعية على الالتزام بالقوانين والمعايير المتعلقة بحماية البيانات، مما يعزز ثقة المستخدمين ويضمن استمرارية الخدمات.

---

[1] . عبد السلام على شتا، ابتسام. **المرجع السابق**. ص 32

[2] . عبد السلام على شتا، ابتسام. **المرجع السابق**. ص 32

[3] . عبد السلام على شتا، ابتسام. **المرجع نفسه**. ص 33 -34

2.2.4.3تقنية النسخ الاحتياطي:

النسخة الاحتياطية للبيانات هي نسخة من بيانات النظام أو التكوين أو التطبيق التي يتم تخزينها بشكل منفصل عن النسخة الأصلية. قد تواجه المكتبات أحيانًا أحداثًا غير متوقعة، مثل الكوارث الطبيعية أو الأخطاء البشرية أو الأحداث الأمنية أو تعطُّل النظام. النسخ الاحتياطي للبيانات هو وظيفة مهمة لحماية البيانات بهدف تقليل مخاطر فقدانها بكاملها أو جزئيًا في حالة وقوع أحداث غير متوقعة. وهو يوفر للمكتبات القدرة على استرجاع الأنظمة والتطبيقات بحالتها السابقة المطلوبة.[1]

تُعتبر تقنية النسخ الاحتياطي واحدة من أهم الأدوات الوقائية التي تعتمدها المكتبات الجامعية لحماية بياناتها وأنظمتها من التهديدات السيبرانية. تقوم هذه التقنية على إنشاء نسخ مكررة من البيانات والملفات المهمة وتخزينها في مواقع مختلفة، سواء على خوادم محلية، أجهزة تخزين خارجية، أو في السحابة الإلكترونية. وتتيح النسخ الاحتياطي للمكتبات الجامعية استعادة البيانات بسرعة في حال تعرضها لفقدان أو تلف نتيجة هجمات إلكترونية مثل هجمات الفدية، أو بسبب أعطال تقنية أو كوارث طبيعية. على سبيل المثال، يمكن للنسخ الاحتياطية حماية الكتب الإلكترونية، الأبحاث العلمية، وسجلات المستخدمين من التدمير أو الفقدان غير المتوقع. ولضمان فاعلية هذه التقنية.[2]

تعتمد المكتبات على جداول زمنية دورية لإجراء النسخ الاحتياطي (يومي، أسبوعي، أو شهري)، وتُشفَّر النسخ الاحتياطية لضمان أمنها حتى أثناء التخزين. بهذه الطريقة، توفر النسخ الاحتياطي حلاً وقائياً واستراتيجياً يُمكن المكتبات من الحفاظ على استمرارية خدماتها الأكاديمية والبحثية في مواجهة أي تهديد سيبراني يأتي من الداخل أو الخارج.[3]

ومن أجل تحقيق التحول إلى الحفظ الإلكتروني بنجاح، يجب وضع خطط وإجراءات لضمان سلامة الموارد الإلكترونية وحفظها، ويجب أن تتبع المكتبات الجامعية والمؤسسات الأكاديمية إرشادات ومعايير محددة في تنظيم وإدارة الموارد الرقمية، بما يضمن سلامتها والحفاظ عليها. ومن بين هذه الإجراءات ما يلي:

- ويجب أن تتوفر التقنيات اللازمة لتحويل المواد الورقية إلى صيغ رقمية، وتخزينها وحفظها بشكل آمن ومنتظم.

---

[1] . بن شهيدة، محمد. **تكنولوجيا المعلومات والاتصالات في المكتبات الجامعية: الاوعية الالكترونية كحل لتحديات الحفاظ على الموارد والتحديات المستمرة**. طبعة، 01. تيارت. ألفا للوثائق للنشر والتوزيع، 2024. ص20

[2] . بن شهيدة، محمد. **المرجع السابق**. ص 22

[3] . الهيئة الوطنية للأمن والسلامة المعلومات. **سياسة النسخ الاحتياطي**. متاح على الرابط: https://nissa.gov.ly تم الاطلاع بتاريخ: 06-01- 2025 على 19.35

- ضمان الوصول الى المعلومات بسهولة.
- توفر البنية التحتية التقنية اللازمة، وتدريب الكوادر الفنية والإدارية على استخدام هذه الأدوات بشكل فعال.
- كما يتطلب التحول إلى الحفظ الإلكتروني اتخاذ إجراءات لحماية المواد الرقمية من الفقدان أو التلف، من خلال استخدام النسخ الاحتياطية والحفظ في أماكن آمنة[1].

وبالتالي يعتبر التحول من الحفظ التقليدي إلى الحفظ الإلكتروني تطورًا هائلا في مجال الحفظ والإدارة الرقمية للموارد المعلوماتية. ففي الماضي، كانت الموارد المعلوماتية تحفظ على شكل أوراق وثائق مطبوعة وكتب ومجلات، ويتم الاحتفاظ بها في مكتبات وأرشيفات، وكان ذلك يتطلب جهدًا كبيرا للحفاظ عليها وتخزينها بشكل سليم.

ويوفر الحفظ الإلكتروني أيضًا ميزات إضافية مثل:

- الاحتفاظ بالمعلومات لفترات طويلة بدون تدهور.
- التحديث السريع للموارد المعلوماتية، وتوفير مساحة تخزين أكبر.
- التخلص من الأوراق والوثائق المطبوعة التي تشغل مساحة كبيرة وتتطلب صيانة دورية.

وعلى الرغم من فوائد الحفظ الإلكتروني، إلا أنه يتطلب الاهتمام بالعوامل الأمنية والخصوصية للمستخدمين وحماية المعلومات من الاختراقات الإلكترونية. لهذا يعتبر الحفظ الإلكتروني من أهم التحديات التي تواجه المكتبات الجامعية في الوقت الحالي، حيث تعتمد المكتبات على تقنيات التخزين والاسترجاع الإلكترونية[2]

للحفاظ على الموارد المعرفية وتوفير الوقت والجهد. ومع ذلك، فإن هناك عدة تحديات ومتطلبات يجب مراعاتها لضمان نجاح هذا النوع من الحفظ. من بين هذه التحديات والمتطلبات،[3] نذكر ما يلي:

- تحديات الأمان والحفاظ على خصوصية المستخدمين والمحتويات.
- وضمان الوصول الشامل والمتساوي لجميع المستخدمين.
- وضمان الحفاظ على جودة الموارد وعدم تدهورها مع مرور الوقت.

---

[1] . بن شهيدة، محمد. **المرجع نفسه**. ص 25

[2] . الهيئة الوطنية للأمن والسلامة المعلومات. **سياسة النسخ الاحتياطي**. متاح على الرابط: https://nissa.gov.ly تم الاطلاع بتاريخ: 06-01- 2025 على 19.35

[3]. عبد الدايم أحمد الحداد، نبيلة. **المرجع السابق**. ص54

- التحديات المالية المتعلقة بتكاليف الحفظ الإلكتروني وصيانته وتحديثه[1].
- يتطلب الحفظ الإلكتروني في المكتبات الجامعية العمل على توفير البنية التحتية اللازمة للتخزين والاسترجاع الإلكتروني.
- توفير الكفاءات اللازمة للمكتبيين للتعامل مع التكنولوجيات المختلفة المستخدمة في هذا المجال، فضلاً عن العمل على تطوير الخطط الاستراتيجية اللازمة لضمان استدامة الحفظ الإلكتروني وتحديثه بشكل دوري[2].

3.4.3تدريب المستخدمين على الأمن السيبراني:

ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني ومن بين الضوابط والتدابير التي يجب على المكتبة أن تستعملها هي:

- يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دوريا وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية لألمن السيبراني.
- يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك: التعامل الأمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني[3] التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. التعامل الأمن مع خدمات تصفح الانترنيت، والتعامل الآمن مع وسائل التواصل الاجتماعي.
- يجب توفير المهارات المتخصصة والتدريب الإلزام للعاملين في المجالات الوظيفية ذات العالقة المباشرة بالأمن السيبراني في الجهة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك،

[1] . الهيئة الوطنية لأمن السيبراني. **الضوابط الأمن السيبراني**. متاح على الرابط: http://Nca.gov.Sa تم الاطلاع عليه بتاريخ: 06-01-2025. على 20:05

[2] . الهيئة الوطنية لأمن السيبراني. **الضوابط الأمن السيبراني**. متاح على الرابط: http://Nca.gov.Sa تم الاطلاع عليه بتاريخ: 06-01-2025. على 20:05

[3] . الهيئة الوطنية لأمن السيبراني. **المرجع نفسه**

موظفو الإدارة المعنية بالأمن السيبيراني، الموظفون العاملون في تطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة الوظائف الإشرافية والتنفيذية.[1]

5.3 تحديات الأمن السيبيراني في المكتبات الجامعية

تواجه المكتبات الجامعية في ظل التحول الرقمي العديد من التحديات السيبرانية التي تهدد سلامة معلوماتها وخدماتها الإلكترونية، ومن أبرز التحديات نذكر مايلي. ومن أبرز هذه التحديات:

1.5.3نقص الخبرات والكفاءات في مجال الأمن السيبيراني

مع التقدم التكنولوجي المتسارع، أصبحت المكتبات الجامعية تعتمد بشكل كبير على النظم الرقمية لإدارة مواردها وخدماتها. هذا التحول الرقمي يجعلها عرضة لمجموعة من التهديدات السيبرانية التي تهدد سرية المعلومات، سلامة الأنظمة، واستمرارية تقديم الخدمات. ومن بين أبرز التحديات التي تواجه المكتبات الجامعية في تعزيز الأمن السيبراني هو نقص الخبرات والكفاءات المتخصصة في مجال الأمن السيبراني. حيث نجد المكتبات الجامعية تتعامل مع كميات هائلة من البيانات الحساسة، بما في ذلك بيانات الطلاب والموظفين والأبحاث الأكاديمية. حماية هذه البيانات من الاختراق أو الفقدان يعتبر أمرًا حيويًا لضمان سمعة المؤسسة والحفاظ على الثقة بين المستفيدين[2].

ومن بين أسباب نقص الكفاءات في الأمن السيبيراني:

- ندرة المتخصصين:مع تزايد الطلب على خبراء الأمن السيبراني في مختلف القطاعات، تعاني المكتبات الجامعية من منافسة شديدة مع القطاع الخاص والحكومي لجذب هذه الكفاءات.
- محدودية الميزانيات:غالبًا ما تكون الموارد المالية للمكتبات الجامعية محدودة، مما يجعل من الصعب توظيف خبراء متخصصين أو تدريب الموظفين الحاليين في مجال الأمن السيبيراني.
- قلة البرامج التدريبية المتخصصة:نقص الدورات التدريبية أو البرامج التعليمية التي تركز على الأمن السيبراني في سياق المكتبات يزيد من الفجوة في الكفاءات.[3]:

---

[1] . التيماني،مداخل زيد عبد الرحيم،. **واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبيراني. مجلة الخدمة الاجتماعية**، العدد 67، 2021.ص23

[2] . رايس، شيماء؛ فريحة ، محمد كريم. **الحضور الرقمي للمكتبات العامة في الفضاء السيبيراني من وجهة نظر مسيري المنصات التفاعلية: استطلاع اراء القائمين على حسابات المكتبات العامة الجزائرية بموقع فيسبوك**. مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–. المجلد، 35. العدد، 01، 2021. ص 1116

[3]. بن سيدهم، حرية. **الأمن الفضائي السيبيراني: التحديات والحلول**. مجلة الجزائرية للأمن الإنساني. المجلد، 05. العدد، 02، 2020. ص 100- 101

- الاعتماد على الحلول التقليدية:الكثير من المكتبات لا تزال تعتمد على أدوات وإجراءات تقليدية للحماية، مما يجعلها غير مهيأة للتعامل مع التهديدات الحديثة. ومن بين أثار نقص الكفاءات في تعزيز الأمن السيبيراني
- زيادة خطر الاختراقات: تصبح المكتبات أكثر عرضة للهجمات السيبرانية مثل سرقة البيانات، أو تعطيل الأنظمة[1].

2.5.3تسريب البيانات الشخصية:

لم تشهد المكتبات التقليدية إنتهاكات كثيرة فيما يخص البيانات الشخصية في البيئة الرقمية،وإن حصل ذلك فمن السهل إكتشاف الاعتداء وتطبيق القوانين اللازمة والتي نصت عليها التشريعات بوضوح ودون إلتباس مقارنة بما يحصل اليوم في بيئة أكثر ما يميزها هو السرعة الفائقة في إنتشار المعلومة[2].

كما أن الوسائل التكنولوجية الحديثة ساهمت وبشكل رهيب في إنتشار هذه الاعتداءات. ومساهم أسياسي في الاعتداء على حقوق الغير وتسريب البيانات خاصة البيانات الشخصية، في حين أن ذلك يكون بطريقة غير مباشرة وبوعي أو دون وعي من مستعمل هذه الوسائل أو التقنيات الحديثة.

كما أن المستفيد من المكتبة التقليدية يقوم باستعارة وعاء المعلومات من اجل القراءة والمطالعة ومن ثم يقوم بإعادته للمكتبة لتقوم هي بعد ذلك بإعارته لشخص آخر. بينما في المكتبة الرقمية فالأمر مختلف تماما، فالمستفيد يقوم بعملية إنزال مصدر المعلومات الرقمي من موقع المكتبة على الشبكة مما يخوله ملكيته الكاملة.[3]

3.5.3نقص الوعي الأمني لدى المستخدمين والموظفين في المكتبات الجامعية

أحد أكبر التحديات التي تهدد حماية المعلومات أن يفتقر المستخدمون أو العاملون إلى المعرفة الكافية بممارسات الأمان الرقمي، يصبحون أكثر عرضة للقيام بسلوكيات تعرض أنظمة المكتبة وبياناتها للخطر.

وفي مايلي نذكر أبرز الحالات وهي كالآتي:

- إستخدام كلمات مرور ضعيفة أو مشاركتها: كثير من المستخدمين والموظفين قد يستخدمون كلمات مرور ضعيفة أو يسهل تخمينها، أو قد يشاركون كلمات المرور مع الآخرين دون إدراك المخاطر.

---

[1]. بن سيدهم، حرية. **المرجع السابق**.ص 100- 101

[2] . بوعيشة، بوغفالة؛ بلعيور، محمدنذير. **حماية الملكية الفكرية الأدبية والفنية في البيئة الرقمية في ظل التشريع الجزائري**. المجلد، 05. العدد، 05، 2020. ص 46

[3] . بوعيشة، بوغفالة؛ بلعيور، محمدنذير. **المرجع السابق**. ص 46

- فتح روابط أو مرفقات مشبوهة: عدم وعي المستخدمين بخطر رسائل البريد الإلكتروني الخادعة يجعلهم عرضة للهجمات الإلكترونية[1].
- إستخدام الأجهزة الشخصية غير المحمية: يعتمد بعض المستخدمين والموظفين على أجهزتهم الشخصية للوصول إلى أنظمة المكتبة، دون التأكد من حمايتها ببرامج مكافحة الفيروسات أو التحديثات الأمنية.
- ترك الأجهزة مفتوحة دون رقابة: يمكن أن يؤدي ترك الأجهزة مفتوحة أو تسجيل الدخول في الأماكن العامة إلى وصول غير مصرح به.
- قلة التوعية بالهجمات السيبرانية: قد لا يكون لدى المستخدمين والموظفين فهم كافٍ لأنواع الهجمات الحديثة وكيفية الحماية منها

– عدم تأمين نظم الحاسبات والمعلومات يعرض ممتلكات المكتبة وبياناتها للتخريب والتدمير خاصة في حالة عدم وجود نظم حفظ بديلة[2].

4.5.3تطور التهديدات السيبرانية:

مع الاعتماد المتزايد على التكنولوجيا الرقمية في المكتبات الجامعية، أصبحت الأنظمة والمعلومات المخزنة عرضة للتهديدات السيبرانية المتطورة مثل: الهجمات الإلكترونية وسرقة البيانات. يمكن أن تؤدي هذه التهديدات إلى اختراق قواعد البيانات الأكاديمية، مما يعرض الأبحاث والوثائق العلمية للخطر أو يعيق الوصول إليها. على سبيل المثال، يمكن أن تستهدف الهجمات البرمجيات الخبيثة (Malware) أنظمة المكتبات، مما يؤدي إلى تعطيل الوصول إلى الموارد الرقمية مثل المقالات والدوريات العلمية. بالإضافة إلى ذلك، قد يستغل المهاجمون الثغرات الأمنية للحصول على بيانات حساسة عن الطلاب والباحثين، مما يهدد خصوصيتهم. للتصدي لهذه التحديات، يجب على المكتبات الجامعية تبني تقنيات أمان متقدمة، مثل التشفير وجدران الحماية، وتوفير تدريب دوري للموظفين للتعامل مع المخاطر الإلكترونية. ومن أهم التحديات السيبرانية التي يمكن أن تواجه المكتبات الجامعية في تأمين المعلومات[3]،

---

[1]. بوقرص، ساعد. **الأمن السيبيراني: مخاطر وتحديديات وتحديات تتطلب ممارسات وتوصيات وإستراتيجيات خاصة.** Journal of social protection research. المجلد، 03. العدد،01، 2022.ص 70

[2]. بوقرص، ساعد. **الأمن السيبيراني: مخاطر وتحديديات وتحديات تتطلب ممارسات وتوصيات وإستراتيجيات خاصة.** Journal of social protection research. المجلد، 03. العدد،01، 2022.ص 70

[3]. بن سيدهم، حرية. **المرجع السابق**.ص 100- 101

5.5.3مقاومة التغيير في المكتبات:

تعد المكتبات الجامعية ركيزة أساسية لدعم البحث العلمي والتعليم من خلال توفير مصادر رقمية ومادية متنوعة. ومع تزايد التهديدات السيبرانية، أصبحت الحاجة لتعزيز الأمن السيبراني في هذه المكتبات ضرورة ملحة. ومع ذلك، يبرز تحدي مقاومة التغيير كعقبة رئيسية أمام تطبيق الحلول الأمنية الحديثة. يُعزى هذا التحدي إلى عوامل متعددة تتعلق بالعامل البشري والتنظيمي، مما يتطلب استراتيجيات شاملة لتجاوزها.

تعتمد المكتبات الجامعية على أنظمة رقمية متطورة لتخزين البيانات وإدارة العمليات اليومية. ومع تزايد الهجمات السيبرانية مثل سرقة البيانات أو تعطل الأنظمة، أصبح التكيف مع التغيرات الأمنية أمراً حتمياً لضمان حماية المعلومات الحساسة والحفاظ على استمرارية الخدمة. يتطلب هذا التغيير تبني تقنيات جديدة، تطوير سياسات أمنية، وتغيير سلوكيات المستخدمين، وهو ما يواجه أحياناً مقاومة قوية. ومن الأسباب التي تجعل المكتبات الجامعة إلى عدم تبني تقنيات جديدة نذكر ما يلي:

1. يشعر الموظفون والمستخدمون بالقلق من فقدان السيطرة أو التعامل مع تقنيات لا يفهمونها بشكل كامل.
2. يميل البعض إلى الحفاظ على الوضع الراهن لتجنب الجهد اللازم لتعلم أنظمة أو سياسات جديدة.
3. غياب الفهم الكافي لأهمية التغيير ودوره في تعزيز الأمن السيبراني يؤدي إلى تقليل تقبله.
4. يشعر بعض العاملين أن التغييرات الأمنية تفرض عبئاً إضافياً دون توفير الموارد الكافية لدعمها.
5. في بعض المكتبات، قد تكون الثقافة التنظيمية غير مهيأة لتقبل التغيير بسبب هياكل إدارية جامدة[1].

[1]. برباش، توفيق. **إستراتيجيات التعامل مع مقاومة التغيير: قراءة تحليلية في تجارب مؤسسات رائدة.** مجلة التمويل والإستثمار والتنمية المستدامة. المجلد، 10. العدد، 01، 2025.ص 538

خلاصة الفصل:

وكخلاصة لما سبق، نستنتج أن تحقيق الأمن السيبيراني عامة وفي المكتبات الجامعية خاصة أصبح حتمية في وقتنا الراهن، خصوصا مع التوجهات الجديدة الناتجة عن التحول الرقمي وظهور المعلومات كمورد أساسي في المؤسسة تساعد في آداء وظائفها وتقديم خدماتها لجميع شرائح المجتمع دون قيود وإتخاذ قراراتها. كما أن إعتماد المكتبات الجامعية على النظم الإلكترونية في إدارة مواردها وخدماتها جعلها أكثر عرضة لمخاطر الأمن السيبيراني مثل: الإختراقات والتجسس، وإنتهاك خصوصية البيانات وغيرها.

ولمواجهة مخاطر وتهديديات الفضاء السيبيراني كان على المكتبات تبني إستراتيجيات وتقنيات لإدارة مخاطر الأمن السيبيراني لضمان أمن وسرية البيانات وإستمرارية العمل في المؤسسة، وهذا الأخير لن يتأتى إلا من خلال الإمتثال إلى سياسات وأطر وآليات واضحة تضمن سلامة وحفظ البيانات وتحقق الشفافية داخل المؤسسة.

الفصل الرابع:

دور حوكمة المعلومات في التقليل من مخاطر الأمن السيبراني في المكتبات الجامعية

الفصل الرابع: دور حوكمة المعلومات في التقليل من مخاطر الأمن السيبراني في المكتبات الجامعية

تمهيد:

بعد التعرف على حوكمة المعلومات ومبادئها ومخاطر وتهديدات الأمن السيبراني والتحديات المترتبة عنه، يناقش الفصل الرابع؛ علاقة حوكمة المعلومات بالأمن السيبراني، ومكانتهما في المكتبات الجامعية، وفوائد تطبيق حوكمة المعلومات للتقليل من المخاطر والتهديدات المحتملة، كما تم التطرق إلى أطر حوكمة المعلومات لإدارة مخاطر الفضاء السيبراني وأثر تطبيقها في المكتبات الجامعية، وفي الأخير الوقوف على أبرز تحدياتحوكمة المعلومات لإدارة مخاطر الأمن السيبراني في المكتبات الجامعية.

1.4مكانة حوكمة المعلومات والأمن السيبراني في المكتبات الجامعية

1.1.4حوكمة المعلومات ومخاطر الأمن السيبراني

تعد حوكمة المعلومات إطار إستراتيجيا يهدف إلى تنظيم إدارة المعلومات داخل المؤسسات من خلال وضع السياسات والمعايير والإجراءات التي تضمن الإستخدام الفعال والأمن للمعلومات. أما الأمن السيبيراني فهو مجموعة من التدابير والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية والإختراقات. وتتجلى العلاقة بينها في أن تطبيق ممارسات حوكمة المعلومات يسهم في تعزيز مستوى الأمن السيبيراني في المؤسسة.ويتأتى هذا من خلال وضع سياسات واضحة لإدارة المعلومات وتحديد المسؤوليات وتطبيق ضوابط الوصول يمكن تقليل المخاطر المرتبطة بالهجمات السيبرانية.[1]

في سياق المكتبات الجامعية تصبح هذه العلاقة أكثر أهمية نظرلحجم البيانات الأكاديمية والعلمية التي يتم تخزينها وإدارتها. فحوكمة المعلومات في المكتبات الجامعية تضمن تنظيم البيانات الرقمية، وحماية حقوق الوصول إليها، وأيضا ضمان الإمتثال للسياسات الأمنية. من جهة أخرى يعزز الأمن السيبيراني حماية قواعد بيانات المكتبات الأكاديمية، والمكتبات الرقمية والأنظمة الإلكترونية المستخدمة فيالبحث والتعلم. ذلك أن تطبيق سياسات حوكمة المعلومات يمكن المساهمة في تقليل المخاطر السيبرانية التي تهدد سرية وسلامة البيانات البحثية، والملفات الخاصة بالطلاب والباحثين[2]. كما تضمن إستمرارية الخدمات الرقمية المقدمة على شبكة الانترنت دون التعرض للإنتهاكات السيبرانية.

---

[1] . نابتي، محمد صالح. **الوصول الى المعلومات العلمية والتقنية: واقع المكتبات الجامعية الجزائرية**. مجلة المكتبات والمعلومات. المجلد، 04. العدد، 01، 2011.ص 56

[2] . بومعرافي، بهجة. عقابو، خالد. **حماية الكيانات الرقمية وضمان استمراريتها من خلال استراتيجيات أمن المعلومات بالمستودعات الرقمية الجامعية: مستودع جامعة محمد خيضر بسكرة نموذجا**. مجلة المعيار. المجلد، 27. العدد، 03، 2023. ص 757

وبالتالي فإن التكامل بين حوكمة المعلومات والأمن السيبيراني في المكتبات الجامعية لا يقتصر فقط على حماية المعلومات، بل يمتد إلى تعزيز كفاءة الأداء وضمان إستدامة الخدمات الأكاديمية في بيئة رقمية آمنة خاصة في ظل التهديدات الأمنية التي تتعرض لها.

على ضوء ما سبق، نلاحظ أن بيئة المكتبات الجامعية تتميز بالديناميكية والإنفتاح، الأمر الذي يجعلها عرضة للعديد من التهديدات، وتتمثل هذه التهديدات في مايلي:

1. مشركة الموظفين في إستخدام نفس كلمة السر للدخول إلى النظام أوالعبث بمحتوياته.
2. عدم الفصل بين المهام والوظائف في المؤسسة
3. ضعف وعدم كفاءة النظم والتطبيقات.
4. عدم وجود سياسات وبرامج محددة ومكتوبة لأمن المعلومات في المؤسسة.
5. عدم الإهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية للموظفين.
6. ضعف الوعي الأمني والتقني عندالمكتبيين، هذا الأمر ساهم في غياب فحص ومراجعة الأنظمة والتطبيقات[1].

2.4 فوائد حوكمة المعلومات على مخاطر الأمن السيبيراني في المكتبات الجامعية

تزداد أهمية التكامل المكتبات الجامعية بين حوكمة المعلومات والأمن السيبيراني نظرا للتحول نحو الأرشفة الرقمية والمكتبات الالكترونية، حيث تلعب حوكمة المعلومات دور رئيسيا في حماية البنية التحتية الرقمية لهذه المكتبات، وتظهر فوائد حوكمة المعلومات على مخاطر الأمن السيبراني في مجموعة من العناصر كالتالي:

- تطبيق سياسات صارمة للوصولإلى الأنظمة الإلكترونية، وتشفير البيانات.
- إعتماد إجراءات تحقق قوية لتقليل المخاطر السيبرانية.
- الإمتثال للقوانين المحلية والدولية المتعلقة بحماية المعلومات، مما يقلل من المخاطر القانونية المحتملة المرتبطة بانتهاك البيانات أو فقدانها. [2]

[1] . بومعرافي، بهجة. عقابو، خالد. **المرجع السابق**. ص 757

[2] . بدر، أحمد. **المرجع السابق**. ص 332

- يؤدي التكامل بين حوكمة المعلومات والأمن السيبيراني إلى تحسين إستجابة المكتبات الجامعية للهجمات الالكترونية، من خلال توفير خطط لإستمرارية العمل والتعافي من الأزمات السيبرانية.
- تضمن سياسات الحوكمة الإحتفاظ بنسخ إحتياطية من البيانات الأكاديمية، وتقللإحتمالية التعرض للهجمات والمخاطر السيبرانية.

تعزز ثقافة الأمن السيبيراني داخل المؤسسةوتضمن تبني نهج منظم ومستدام لحماية المعلومات والبنية التحتية الرقمية الأمر الذي يسهم في المحافظة على إستدامة الخدمات المكتبية والبحثية.

كماأن حوكمة المعلومات تفرض تنفيذ برامج توعية وتدريب دوري للمستخدمين حول ممارسات الأمن السيبيراني، ومن أبرز البرامج مايلي:

- كيفية التعامل مع محاولات التصيد الالكتروني وتأمين الحسابات.
- كلمات المرور والسرية.
- طرق وليات حماية الأجهزة الشخصية عند الاتصال الشبكي.
- توظيف تقنيات الحماية الحديثة.[1]

3.4 أطر حوكمة المعلومات للتقليل من مخاطر الأمن السيبيراني

فرضت التطورات والتغيرات الحديثة في المكتبات نحو التوجه إلى تطبيق الحوكمة لضمان تحقيق أفضل الممارسات والسياسات مع الحفاظ على أمن وسلامة البيانات وجودة الخدمات، خصوصا أمام تصاعد مخاطر وتهديدات المتعلقة بالأمن السيبراني.

وفي هذا الإطار ومع تزايد أهمية وحتمية تطبيق الحوكمة الإلكترونية لتجاوز التحديات لجأت العديد من المكتبات ومراكز المعلومات إلى ضرورة تبني وإستخدام أطر الحوكمة العالمية مثل: COBBIT, ITIL, CMMI, COSO, ISO/EIC 38500،بهدف تحسين فعالية وشفافية العمليات التنظيمية وإتخاذ القرارات، حيث تساهم هذه الأطر من خلال المعايير والإرشادات التي تتضمنها تحقيق الأهداف الإستراتيجية وتعزيز تطبيق السياسات[2].

---

[1] . أبو موسى، أحمد عبد السلام. **مخاطر أمن نظم المعلومات المحاسبية الالكترونية: دراسة ميدانية على المنشآت السعودية.** مجلة الإدارة العامة. المجلد، 44. العدد، 03، 2024. ص 55

[2] . زيوش، زيوش. تيتلة، سارة. **نحو حوكمة الكترونية أفضل في المكتبات ومراكز المعلومات: دراسة تحليلية مقارنة بين لطار COBIT وباقي الأطر**. مجلة المعيار. المجلد، 29. العدد، 01، 2024. ص892

ولتطبيق أفضل ممارسات الحوكمة المعلومات ومن أجل فهم أعمق لهذه الأطر سوف يتم التطرق إلى أهم المعلومات الأساسية حول هذه الأطر، مميزاتها ومجالات تركيزها:

1.3.4إطار COBIT:

يعرف إطار COBIT بأنه إطار لحوكمة وإدارة تقنية المعلومات يساعد المؤسسة على تحقيق القيمة المثل من إستخدام تقنية المعلومات من خلال الموازنة بين تعظيم المنافع المتحققة وتحسين إدارة المخاطر والإستخدام الفعال للموارد، تم إصداره كدليل إرشادي عام 2019 بهدف تمكين المؤسسات في تحصين قدرتها عل تلبية إحتياجات المستفيدين وتحقيق المرونة والسرعة في العمل. شهد الإطار ثلاث تطورات رئيسية وهي:

1. تحسين نموذج النضج لعمليات حوكمة تقنية المعلومات، بما يسهم في رفع مستوى الآداء وتحسين ممارسات الحوكمة.

2. إعادة صياغة المبادئ الأساسية لحوكمة تقنية المعلومات؛ تو توسيعها من خمسة مبادئ إلى ستة.

3. إضافة أهداف جديدة؛ إدارة البيانات، إدارة البرامج وإدارة أنشطة الضمان[1].

1.1.3.4 آليات إطار COBIT

يوفر الإطار النهج السليم لتنفيذ عمليات حوكمة تكنولوجيا المعلومات، حدد 34 عملية رقابية على تكنولوجيا المعلومات تتضمن أكثر من 300 هدف. تتوزع آليات الإطار في أربع (04) مجالات أساسية وهي:

التخطيط والتنظيم: يوضح المجال كيفية إستخدام تكنولوجيا المعلومات في المؤسسة وذلك من خلال مجموعة من خلال مايلي:

توفير أدوات مساعدة في تنفيذ الأهداف العامة والخاصة للمؤسسة.

تحقيق الموائمة بين الهيكل التنظيمي للمؤسسة ونظام تكنولوجيا المعلومات[2]..

عمليات التخطيط والتنظيم تتم وفق جداول زمنية ويتم دعمها من قبل جميع المستويات الإدارية.

---

[1].Ishlahuddin, Ahmad. **Analysing IT Governance Maturity Level using COBIT 2019 Framework**: **A Case Study of Small Size Higher Education Institute** (**XYZ-edu**). 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020.p. 237

[2]. عزام، وليد حمدان. **دور ليات حوكمة تكنولوجيا وفق إطار COIT في تعزيز ثقة المستثمري بالقوائم المقدمة: دراسة ميدان عل عينة من المصارف العراقية الخاصة**. مجلة الريادة للمال والأعمال. المجلد 04، العدد 04، 2023.ص140

لجان مجلس الإدارة يجب أن تملك الخبرة والمعرفة اللازمة حول تكنولوجيا المعلومات[1].

الإمتلاك والتنفيذ:

- تحديد المتطلبات الخاصة بتكنولوجيا المعلومات وتنفيذها مع الحفاظ على موثوقية وأمن المعلومات.
- التغيرات الحالية التي تحدث في أنظمة التكنولوجيا وصانتها من أجل إستمرارية دورة حياة أنظمة تكنولوجيا المعلومات.

التوصيل والدعم: يقصد به توصيل تكنولوجيا المعلومات داخل أنشطة المؤسسة وتنفيذ التطبيقات الخاصة به ودعم العمليات، لتكون فاعلة وقادرة على تنفيذ الأنشطة والخدمات.

المتابعة والتقييم: تتحدد أهداف المجال في مجموعة من العناصر، وهي:

- التحقق من مدى إنسجام أنظمة تكنولوجيا المعلومات مع الخطة الإستراتيجية للمؤسسة.
- إجراء تقييم مستقل للكفاءة وفعالية أنظمة تكنولوجيا المعلومات ومدى قدرة الأنظمة على تحقيق الأهداف وعمليات الرقابة.
- ضمان تحقق الإشراف الإداري على عمليات الرقابة في المؤسسة[2].

2.3.4 إطار COSO

إطار عمل الرقابة الداخلية؛ الإطار المتكامل COSO: هو مجموعة الممارسات التي تلزم المؤسسة بالنزاهة والقيم الأخلاقية، تم نشره من قبل لجنة المنظمات الراعية التابعة تريدواي COSO. يهدف الإطار إلى تحقيق مجموعة من الأهداف وهي كالتالي:

- ضمان أن العمليات ذات كفاءة وفعالية .
- ضمان ان الأصول قد تم إتخا الغجراءات اللازمة لحمايتها.
- ضمان أن العمليات تتم وفقا للأنظمة والتشريعات والقوانين[3].

---

[1]. عزام، وليد حمدان. **المرجع السابق**.ص140

[2]. عزام، وليد حمدان. **المرجع نفسه**.ص140

[3]. الأكاديمية الدولية للوساطة والتحكيم. **أنظمة الرقابة الداخلية**. العدد 05، أغسطس 2022.ص 02-03

1.3.3.4 عناصر الرقابة الداخلية وفق إطار لجنة COSO

يعتمد نموذج الرقابة الداخلية في تحقيق أهدافه على خمسة (05) عناصر أساسية تتداخل فيما بينها لتشكل إطار متكامل وفعال للرقابة الداخلية، وتتمثل في نفس الوقت قاعدة أساسية لقيام نظام سليم وفعال للرقابة الداخلية في المؤسسة،وهي كالآتي:

1.بيئة الرقابة: وهو عنصر مهم في يتعلق بأخلاقيات المؤسسة ومستو الوعي الرقابي لد موظفيها، بما في ذلك الإنظباط والنزاهة والقيم الأخلاقية والكفاءة، وتتحدد مبادئها في العناصر التالية:

- الإلتزام بالنزاهة والأخلاق في العمل.
- الإشراف على الرقابة الداخلية من قبل مجلس الإدارة.
- الهياكل، خطوط الإبلاغ، والمسؤوليات المناسبة في السعي لتحقيق الأهداف التي وضعتها الإدارة بإشراف المجلس.
- الإلتزام بجذب الأفراد ذوي الكفاءة وتطويرهم والإحتفاظ بهم بالتوافق مع الأهداف.
- محاسبة الأفراد عن مسؤولياتهم[1].

2. تقييم المخاطر: وهي الجهود التي تليها المؤسسة لتحديد النمخاطر والتهديدات التي تعترض أداء نشاطها داخلية كانت أو خارجية وبالتالي تهدد إستمراريتها[2]. تظهر مبادئ تقييم المخاطر في مايلي:

- تحديد الأهداف بشكل واضح لتحديد المخاطر وتقييمها.
- تحديد وتحليل المخاطر لتحديد كيفية إدارتها.
- النظر في إمكانية إرتكاب الإحتيال.
- تحديد وتقييم التغييرات التي يمكن أن تؤثر بشكل كبير في الرقابة الداخلية[3].

---

[1]. سلمان، رائد فاضل حمد. **مدى إلتزام البنوك التجارية بتطبيق إجراءات الرقابة الداخلية وفق إطار COSO المتكامل: دراسة تطبيقية في مصارف البنوك التجارية الخاصة**. مجلة الجامعة العراقية. العدد 51، 2021.ص 263

[2]. كشرود، بشير. محيوت، نسيمة. **الإطار المتكامل للرقابة الداخلية COSO–IC وأثره على الرقابة الداخلية في الجزائر**. مجلة جديد الاقتصاد. العدد، 11، ديسمبر 2016.ص226

[3]. سلمان، رائد فاضل حمد. المرجع نفسه.ص263

- **3. الأنظمة الرقابية:** وهي السياسات والإجراءات الموضوعة لضمان تحقيق أهداف المؤسسة بالإضافة من التأكد من تنفيذ الإستراتيجيات المتبناة مواجهة المخاطر بفعالية، وتشمل المبادئ التالية:
- إختيار الإجراءات الرقابية وتطويرها والتي قد تساعد عل تخفيف المخاطر إل مستو مقبول.
- إختيار أنشطة الرقابة العامة وتطويرها عل تقنية المعلومات.
- نشر أنشطة الرقابة عل النحو المحدد في السياسات والإجراءات ذات الصلة[1].

4. المعلومات والإتصال: هي عنصر جوهري لتحقيق أهداف المؤسسة، وتشمل المبادئ التالية: إستخدام معلومات ذات صلة وجودة لتطبيق الرقابة الداخلية، والتواصل الداخلي والخارجي لتفعيل الرقابة.

5. المراقبة: هي رقابة نظام الرقابة على مدار الوقت، وتتحدد مبادئها في: إجراء تقييم مستمر وأو منفصل لمكونات الرقابة الداخلية، والتقييم والإبلاغ عن جوانب القصور في الرقابة الداخلية[2].

إلى جانب الأطر المذكورة، يوجد أطر أخرى مثل ITIL, CMMI,ISO/EIC 38500 والتي تسعى إلى تحسين إدارة تكنولوجيا المعلومات وتطبيق أفضل ممارسات الحوكمة المعلومات ،ومن أجل فهم أعمق لهذه الأطر سوف يتم التطرق إلى أهم المعلومات الأساسية حول الجهات إصدار هذه الأطر، الإصدارات المختلفة لكل منها، ومجالات تركيزها.[3]

3.3.4 معيار ISO/IEC 27001

تعتبر المعلومات أحد أصول المؤسسة القيمة والهامة والتي تؤثر بشكل مباشر على آدائها وإستدامتها، لذلك تحرص المؤسسات على توفير الحماية الكافية للمعلومات من المخاطر الداخلية والخارجية من خلال إعتماد سياسيات وأدوات والأطر فعالة للأمن المعلومات.

ومن هذا المنطلق، ظهرت مجموعة من المعايير من أجل إقتباس أفضل الممارسات والتطبيقات لضمان إدارة أمن المعلومات، وأفضل معيار يمكن الإعتماد عليه في مجال أمن المعلومات المواصفة الدولية ISO/IEC27001.

---

[1]. كشرود، بشير. محيوت، نسيمة. **المرجع السابق**.ص226

[2]. الأكاديمية الدولية للوساطة والتحكيم. **المرجع السابق**.03

[3]. زيوش، زيوش. تيتلة، سارة. **المرجع السابق**. ص 896

يعالج المعيار إدارة أمن المعلومات حسيث يرتكز على مفاهيم السرية والسلامة والتوافر، والهدف الأساسي لنظما أمن المعلومات العمل على حماية الخصائص الثلاثة بالنسبة للمعلومات الحساية في المؤسسة، كما تحدد المواصفة الدولية الطريقة الواجب إتباعها من اجل إعداد ووضع نظام إدارة أمن المعلومات[1] وهو كالآتي:

- تعريف نطاق نظام أمن المعلومات.
- تكوين سياسات الإدارة.
- تحديد طرق تحليل المخاطر: تعد طريقIBIOS أحد أبرز الطرق المستعملة لتحليل المخاطر، تختص هذه الأخيرة في تقييم ومعالجة المخاطر المتعلقة بأمن أنظمة المعلومات.
- تعريف، تحليل المخاطر وتقييمها وتحديد المعالجات المطبقة على مختلف المخاطر.
- إثبات إلتزام إدارة المؤسسة في طريقة نظام إدارة أمن المعلومات[2].

الجدول رقم (04): الأطر العالمية التي تربط حوكمة المعلومات والأمن السيبيراني

أطر الحوكمة	جهة الإصدار	الإصدارات	مجالات التركيز
أهداف التحكم في المعلومات والتكنولوجيا ذات الصلة COBIT)	جمعية التدقيق والرقابة على أنظمة المعلومات (ISACA)	- COBIT1 (1996) - COBIT2 (1998) - COBIT3 (2000) - COBIT4 (2005) - COBIT4 (2007) - COBIT5 (2012) - COBIT2019 (2018)	يركز على الامتثال للوائح التنظيمية، ويساعد المؤسسات على زيادة القيمة المستفادة من تكنولوجيات المعلومات، ويمكن من محاذاة استراتيجيات تكنولوجيا المعلومات مع أهداف المنظمة، ويبسط إجراءات تنفيذ الحوكمة.
نموذج نضج القدرات المتكاملِ CMMI	معهد هندسة البرمجيات SEI بجامعة كارنيجي ميلون	- CMMI V.1.1(2002) - CMMI V. 1.2 (2006) - CMMI V. 1.3 (2010) - CMMI V. 2.0	يركز على تحسين القدرات المؤسسية من خلال تحسين العمليات وتقييم الأداء

[1]. فيلالي، أسماء. **دور المواصفة الدولية ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات في المؤسسة**. مجلة إضافات إقتصادية. المجلد، 05، العدد 01، 2021.ص 214-215

[2]. فيلالي، أسماء. **المرجع السابق**.ص 215

	(2018) - CMMI V.3.0 (2023)		
تهدف الى إدارة خدمات تكنولوجيا المعلومات بكفاءة وفعالية من خلال أفضل الممارسات.	- ITIL V1 (1989) - ITIL V2 (2000) - ITIL V3 (2007) - ITIL V4 (2019)	Axelos	مكتبة البنية التحتية لتكنولوجيا المعلومات ITIL
يركز على الرقابة الداخلية وإدارة المخاطر	- Coso 1(1992) - Coso 2(2013)	Tredway Commission	الإطار المتكامل للرقابة الداخلية COSO
يوفر مبادئ توجيهية وإرشادات لحوكمة تكنولوجيا المعلومات على مستوى القيادة.	- ISO/IEC 38500 (2008) - ISO/IEC 38500 (2015) - ISO/IEC 38500 (2024)	المنظمة الدولية لتقييس ISO و اللجنة الكهرو تقنية الدولية IEC	معيار حوكمة تكنولوجيا المعلومات (ISO/ IEC 38500)

في ضوء ما سبق، نخلص أن أطر حوكمة المعلومات عديدة ولكل منها مجال ومبادئ يحدد نهج وسياسة عمل المؤسسة، والجدول الموالي يقدم مقارنة لأطر حوكمة المعلومات وأهدافها والفئة المستهدفة:

الجدول رقم (05): مقارنة أطر حوكمة المعلومات

Framework	Goals	Targeted Audiences
CMII	Provides guidance for process development	System and application development leader
COSO	mprove supervision of the organization by determining integrated systems	Leaders, management, users, and internal auditors
ISO 20000	A set of process management to produce effective services	Management level
TOGAF	Provide strategies to achieve goals by building	Division/person that are responsible for EA

	enterprise architecture	management
COBIT	Provides IT governance guidelines for business, IT risk, information security and quality assurance	Internal organizations, practitioners, and consultants

المصدر[1]:

4.4 دور حوكمة المعلومات في التقليل من مخاطر الأمن السيبيراني

أدت الزيادة السريعة في استخدام التقنية والانترنيت الى الدخول لمجتمع المعلومات، وأصبحت المكتبات الجامعية تعتمد على أنظمة المعلومات الالكترونية في تنفيذ المهام والوظائف المنوطة بها، والتي تمثل نتائجها نقطة الاتصال بين المنظمة والأطراف ذات العلاقة. وتواجه نظم المعلومات في المكتبات الجامعية مخاطر كبيرة يمكن أن تستغل نقاط الضعف والثغرات المعروفة وغير المعروفة على حد سواء في هذه النظم، اذ أشارت الكثير من الدراسات قيمة أعمال الجريمة الالكترونية أصبحت تقدر بحوالي 105 بليون دولار سنويا. بحيث تؤثر مخاطر الأمن المعلومات سلبيا على المكتبات الجامعية وعملياتها وأصولها والعاملين بها وقد تؤدي الى تهديد غيرها من المكتبات، بحيث تهدد سرية ونزاهة ومدى توافر المعلومات المحاسبية التي يتم معالجتها وتخزينها وارسالها وتخزينها أو الإفصاح عنها بواسطة نظم المعلومات المحاسبية الالكترونية، لذلك لجأت العديد من المكتبات الجامعية الى تطبيق حوكمة أمن المعلومات والتي تهدف الى حماية الأصول من مختلف مخاطر المحتملة، من خلال استخدام مجموعة من المعايير الدولية والتي يتم استخدامها على نطاق واسع للتأكد من الوصول لمستوى الأمن المطلوب والكافي.[2]

تعزيز الأمن السيبيراني مرتبط بتحسين حوكمة المعلومات من خلال تبنيها نهجا إستراتيجيا يجمع بين الأطر التنظيمية والتقنيات الحديثة والثقافة المؤسسية للأمن، وتتمثل إحدى الركائز الأساسية لهذا النهج في وضع سياسات واضحة لإدارة البيانات وتحديد من يمكنه الوصول اليها، وكيفية تخزينها ومشاركتها بأمان. كما يجب أن تتكامل حوكمة المعلومات مع إستراتيجيات إدارة المخاطر، بحيث يتم تقييم التهديدات المحتملة بانتظام واتخاذ تدابير استباقية لمعالجتها.

تلعب التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة دورا مهما في تعزيز الأمن السيبيراني عبر الكشف عن الأنشطة المشبوهة والتهديدات المحتملة، مما يتيح الاستجابة الفورية وتقليل الأضرار. بالإضافة الى

---

[1]. Ishlahuddin, Ahmad.Adip.237

[2] . خليفة، أحمد. ضيف الله، محمد هادي. واخرون. **أثر حوكمة تكنولوجيا المعلومات على الحد من المخاطر نظام المعلومات المحاسبي: دراسة ميدانية لعينة من المحاسبين من 2019/09/14 الى 2019/10/30**. مجلة الدراسات المالية والمحاسبية والإدارية. المجلد،08. العدد، 01، 2021. ص 205_207

ذلك فإن تبني معايير الإمتثال الدولية مثل: ISO27001، Nist Cybersecurity Framework يساعد المؤسسات على تحسين ممارساتها وفق متطلبات حماية البيانات في إدارة الأمن السيبيراني وضمان توافقها مع أفضل الممارسات العالمية[1].

ومن الجوانب الحاسمة في حوكمة المعلومات الفعالة تعزيز ثقافة الأمن السيبيراني داخل المؤسسات، وذلك من خلال توفير برامج تدريبية دورية للموظفين لزيادة وعيهم بالمخاطر السيبرانية وأساليب التصدي لها، كما ينبغي على المؤسسات تطوير الخطط استجابة للحوادث السيبرانية لضمان القدرة على التعامل مع الاختراقات بسرعة فعالة، وتقليل تأثيرها على العمليات التشغيلية.[2]

وتعد حوكمة المعلومات عنصر أساسيا من عناصر حوكمة المؤسسات كونها تعرف بأنها ترتيب استراتيجي لأمن المعلومات من خلال رقابة فعالة لاستخدام تقنية المعلومات وتطبيق المساءلة ، وإدارة الأداء، وإدارة المخاطر، يتكون من القيادة والهياكل التنظيمية والعمليات المشاركة في حماية الأصول المعلوماتية، بهدف توفير بيئة رقابية مناسبة للحفاظ على سرية وسلامة وتوافر المعلومات، ودعم العمليات والنظم الخاصة بها، وأيضا حماية المعلومات من المخاطر الأمن السيبيراني وتحديد صلاحية صنع القرار واطار المساءلة للتشجيع على سلوك مرغوب فيه لاستخدام تقنية المعلومات.

وتبرز دور حوكمة المعلومات في العديد من الأدوار والتي تعود بالمنفعة للمكتبات الجامعية خاصة فيما يتعلق بالأمن السيبيراني وتتمثل أهم تلك الأدوار يما يأتي:[3]

- تحديد المخاطر المتعلقة بأمن السيبيراني والعمل على تخفيضها الى مستويات مقبولة.
- الحماية من المساءلة المدنية أو القانونية الناتجة عن عدم دقة المعلومات.
- ضمان وضع سياسة فعالة لأمن المعلومات والالتزام بتلك السياسة.
- إدارة المخاطر بكفاءة وفعالية، وتحسين العمليات.
- الاستجابة السريعة للحوادث المتعلقة بأمن المعلومات.

---

[1] . بارة سميرة. **الأمن السيبيراني في الجزائر: السياسات والمؤسسات**. المجلة الجزائرية لأمن الإنساني. المجلد، 02. العدد، 02،2017. ص 259 _ 261

[2] . بارة سميرة. **الأمن السيبيراني في الجزائر: السياسات والمؤسسات**. المجلة الجزائرية لأمن الإنساني. المجلد، 02. العدد، 02،2017. ص 259 _ 261

[3] . الشيخ يمسن، أحمد. **تطوير مهنة المكتبات: أخصائي المكتبات والمعلومات**. المجلة الأردنية للمكتبات والمعلومات. المجلد،48. العدد، 03، 2013. ص 2013

- توفير مستوى من التأكد على اتخاذ القرارات الحاسمة والهامة لا يستند على معلومات غير صحيحة ومضللة.
- تعمل حوكمة المعلومات على توفير إطار للرقابة لضمان أن المخاطر التي تتعرض لها المكتبات يتم الوصول بها الى المستوى المسموح به[1].
- تأكيد على الاستراتيجيات الأمن التي تتبعها المكتبات الجامعية تتفق مع الأهداف الاستراتيجية.

وفي نفس السياق يمكن القول إن المكتبات أصبحت تعتمد بشكل كبير على الأنظمة الالكترونية لإدارة الموارد والمعلومات الأكاديمية. ومع هذا التحول تزايدت التهديدات السيبرانية التي تهدد أمن المعلومات وسلامة البيانات المخزنة في هذه المكتبات. لذا أصبح من الضروري وضع سياسات أمنية صارمة الى جانب تطبيق تقنيات متكاملة لحماية البيانات وضمان استمرارية الخدمات الرقمية بأمان.[2]

ويقصد بالسياسات الأمنية هي مجموعة من القواعد والممارسات التي تهدف الى تنظيم وحماية البيانات والأنظمة الرقمية من التهديدات المختلفة، سواء كانت داخلية (كسوء استخدام الموظفين للأنظمة)، أو خارجية (مثل الهجمات السيبرانية). [3]وتكمن أهمية السياسات الأمنية في المكتبات الجامعية فيما يلي:

- توفير اطارا تنظيميا للحافظ على سرية المعلومات وسلامة البيانات من المخاطر السيبرانية من خلال وضع قواعد وإجراءات تحكم كيفية إدارة البيانات وحمايتها داخل المكتبات، بهدف ضمان سرية المعلومات وسلامتها في مواجهة الهجمات السيبرانية يشمل هذا الإطار السياسات الأمنية، المعايير التقنية، الإجراءات الوقائية من أجل حماية المصادر الرقمية وسجلات المستخدمين والأنظمة الالكترونية من أي اختراق أو سوء استخدام.[4]
- ضمان استمرارية الخدمات الرقمية أي اتاحة الأنظمة والخدمات الالكترونية في المكتبات الجامعية دون انقطاع حتى في حالة حدوث تهديدات امنية أو اعطال تقنية، من خلال الاعتماد على الأنظمة الرقمية لتوفير خدمات مثل: اتاحة المصادر الأكاديمية، قواعد البيانات الالكترونية، أنظمة الإعارة الالكترونية،

---

[1] . خليفة، أحمد. ضيف الله، محمد هادي. وآخرون. **المرجع السابق**. ص 265

[2] . خليفة، أحمد. ضيف الله، محمد هادي. وآخرون. **المرجع السابق**. ص 265

[3] . الهيئة الوطنية لأمن وسلامة المعلومات National Information Security and Safety Authority. **السياسة الوطنية لأمن وسلامة المعلومات**. ص 65 تاريخ الولوج:13/03/ 2025.على 12:36 متاح على الرابط: https://nissa.gov.ly

[4] . شليل، عبد اللطيف. فيلالي، أسماء. **تهديدات أمن المعلومات وسبل التصدي لها**. مجلة البشائر الاقتصادية. المجلد، 04, العدد، 03، 2019. ص 169

والفهارس الرقمية، وتفعيل حركة الوصول الحر للمعلومات كآلية من اليات الاتصال العلمي الحديث للمكتبات مما يجعل من الضروري وجود سياسات امنية قوية لضمان استمراريتها.[1]

- حماية البيانات الحساسة: من خلال تطبيق مجموعة من الإجراءات والتقنيات التي تهدف الى ضمان سرية وأمان المعلومات المهمة داخل المكتبات ومنع الوصول غير المصرح به أتو تعديل غير قانوني عليها، وتشمل هذه البيانات مثل: معلومات الطلاب والأبحاث الاكاديمية سجلات الاستعارة، البيانات المالية، والمحتوى الرقمي المرخص مما يعزز استمرارية خدمات المكتبات وثقة المستفيدين بها ويضمن الامتثال للمعايير الدولية.[2]

- تحقيق استمرارية التشغيل من خلال خطط الطوارئ والنسخ الاحتياطي المنتظم مما يضمن استعادة البيانات بسرعة في حالة حدوث أي خلل تقني أو هجوم اليكتروني مما يحافظ على استدامة الخدمات الرقمية ويقلل من تأثير الأعطال على المستفيدين.[3]

- تعزز التوعية الأمنية بين الموظفين والمستخدمين مما يقلل من أخطاء البشر التي قد تؤدي الى تهديدات أمنية: وذلك من خلال التدريبات الدورية والارشادات الأمنية بممارسات الأمن السيبيراني بحيث يصبح المستخدمين أكثر وعيا بمخاطر الأمن السيبيراني مما يعزز من ثقافة الأمان الرقمي داخل المكتبات الجامعية.[4]

- توفير بيئة رقمية امنة ومستدامة للمكتبات الجامعية مما يعزز من موثوقية الخدمات المقدمة للطلاب والباحثين. ويتيح ذلك الوصول الامن الى المصادر الأكاديمية والكتب الالكترونية وقواعد البيانات لمستفاديها عن طريق بناء أنظمة معلومات تعمل على اتاحة المعلومات اللازمة لدعم البحث العلمي دون قيود مالية أو قانونية، مع ضمان حماية المعلومات من أي تهديدات خارجية.

ولتنفيذ سياسة أمنية بشكل فعال يتطلب مجموعة من التقنيات والإجراءات وهي كالآتي:

---

[1]. دعي، أحمد. برقان، أحمد. **مساهمة المكتبات الجامعية الجزائرية في حركة الوصول الحر للمعلومات: دراسة حالة المكتبة المركزية لجامعة المسيلة محمد بوضياف**. مجلة قبس للدراسات الإنسانية والاجتماعية. المجلد، 05. العدد،01، 2021. ص 1259 _1260

[2] . اللجنة الفرعية لكتابة السياسات والمعايير المشكلة من قبل لجنة (تنسيق وإدارة النشاط الحكومي باتجاه انشاء حوكم الالكترونية). **وثيقة بعنوان: السياسات ومعايير أمن المعلومات والبيانات**. تاريخ الإصدار: 09 جويلية 2019. ص 27

[3] . موقع الجزيرة نت. **مقال حول: النسخ الاحتياطي وسيلة مثلى لحماية البيانات**. تاريخ الولوج: 13/ 03: 2025. على 13:06 متاح على الرابط: https://www.aljazeera.net

[4] . قتاتلية، خولة.**الأمن السبراني ، التحديات والرهانات**. ملتقى وطني حول: دور الجامعة في تعزيز ثقافة الأمن السيبيراني.جامعة الجزائر 03، 2024.ص15

- تقنيات حماية الشبكات والأنظمة[1]:

1. (جدران النارية FiresWalls): نظرا لانتشار الواسع حاليا لقرصنة المعلومات والتجسس المعلوماتي وذلك بسبب انتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز أو نظام معلوماتي و بدون عناء فور انزال احدى البرامج وخاصة مع وجود ثغرات في الأجهزة والأنظمة، ومن اثار تلك التهديدات التعرض للسرقة أو الاحتيال عن تغيير المعلومات التي يتم إدخالها في النظام أو التغيير المخرجات التي تخرج منه التجسس الصناعي عن طريق تنزيل الأسرار الصناعية من الكمبيوتر الى احدى المؤسسات وارسالها عبر البريد الاليكتروني مباشرة الى منافسيها. الأمر الذي يستدعي ضرورة إيجاد اليات لمواجهتها من بينها الجدران النارية والذي يعتبر هو عبارة عن جهاز أو تطبيق يتم وضعه عند الخادم وعند مصافي الشبكة كل حسب احتياجاته وقد جاءت فكرة الجدار الناري من الطريقة الأمنية المعروفة قديما وهي عبارة عن حفر خندق حول قلعة لمنع أي شخص من الدخول أو الخروج من القلعة. ويمكن تفتيشه من قبل الحراس على القلعة، لذا يقصد بالجدار الناري " مجموعة أنظمة توفر سياسات أمنية بين الأنترنيت والشبكة الخاصة لتصبح جميع عمليات العبور الى الشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصد المستعملين غير المرغوب فيهم، فالجدار الناري الذي يقوم بالتحقق من صلاحية المستعمل المحلي والمستعمل الخارجي، ونظام الدخول والخروج، وتشفير المعلومات، وإجراءات الحماية من الفيروسات.[2] وما يميز الجدار الناري:

- توفير الحماية اللازمة للشبكة والمعلومات.
- التحقق من هوية المستخدمين.
- توفير خدمات التشفير في تكنولوجيا الجدار الناري.
- تخزين العمليات والمعلومات التي تمر من طريق الجدار الناري.
- متابعة المستخدمين للشبكة أو مراقبة المحتوى Content Screening.

وفي نفس السياق تطورت الجدار النارية بشكل متسارع منذ نشأتها حين كانت تقوم بتصفية حركة البيانات اعتمادا على قوانين ومعاملات بسيطة، أما برمجيات الجدران الحديثة، ورغم أنها لا تزال تقوم باستخدام أسلوب فلترة وتصفية البيانات الواردة، فإنها تقوم بعمل ما هو أكثر بكثير مثل انشاء الشبكات الافتراضية الخاصة، ورقابة محتوى البيانات للوقاية من الفيروسات، وحتى أداء نوعية الخدمة Quality of

[1] . بنور، زينب. **الاليات القانونية لحماية قواعد البيانات في البيئة الرقمية**. مجلة القانون والعلوم السياسية. المجلد،10. العدد،02، 2024. ص 65-66

[2] . بنور، زينب. **المرجع السابق**.ص 65-66

service. وهذه الخدمات جميعا تعتمد على ميزة أساسية وهي أن الجدران النارية تقع على طرف الشبكة. وخلال العقد الماضية كانت الجدران النارية ببساطة مجرد أدوات بسيطة تعمل كمنفذ لأنترنيت أو بكلمات أخرى كحراس على طرف الشبكة. والتي تقوم بتنظيم حركة البيانات وحفاظ أمن الشبكة، وقد ظهرت أول الجدران النارية 1980 [1]

وكانت عبارة عن موجات تستخدم في تقسيم هذه الشبكات الى شبكات محلية LAN صغيرة، هوكان هذا النوع من الجدران النارية يضع في مواقعها هذه للحد من انتشار المشاكل التي تواجه جزء من الشبكة. وقم تم استخدام أول الجدران النارية لتحقيق الأمن في أوائل التسعينات. وكانت عبارة عن موجات لبروتوكول IP مع قوانين فلترة كانت تبدوا كالتالي: "اسمح لفلان بالدخول والنفاذ الى الملف التالي"، أو امنع فلان من الدخول الى المنطقة.[2]

وقد كانت هذه الجدران النارية فعالة لكنها نوعا ما محدودة، بسبب صعوبة اتقان وضع قوانين فلترة البيانات ومن الصعب في بعض الأحيان تحديد أجزاء التطبيقات المراد منعها من النفاذ الى الشبكة. وفي أحيان أخرى كانت عناصر الشبكة مثل الموظفين والعاملين ضمنها تتغير، مما يستدعى تغيير القوانين، ولذلك كان الجيل التالي من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل.[3]

والجدران النارية كانت تضع على ما يعرف بالمستضيفات الحصينة Bastion Host وأول جدار ناري من هذا النوع يستخدم الفلاتر وبوابات التطبيقات (البرمجيات البسيطة Proxy) كان من شركة "ديجيتال أكوي منت"، وكان يعتمد على الجدار الناري من شركة Dec حيث ان مختبرات الشبكات التابعة لشركة Dec هي التي وضعت أول الجدران النارية التي انتجتها الشركة. وفي سنة 1991 ابتكر "ماركوس رانوم" في شركة ديجيتال البرمجيات الوسيطة Proxies وأعاد كتابة جزء من الكود الخاص بالجدران النارية، ليتم بعد ذلك طرح منتج Dec sealوالذي كان يتكون في أول الامر من نظام خارجي يدعى حارس البوابة Gatekeeper وهو النظام الوحيد الذي يمكنه مخاطبة الانترنيت.[4]

---

[1] . حزام، فتيحة. **حماية الأنظمة الرقمية بين الأليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 05-20**. مجلة الحقوق والعلوم الإنسانية. العدد، 03، 2020. ص 174 -175

[2] . حزام، فتيحة. **حماية الأنظمة الرقمية بين الأليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 05-20**. مجلة الحقوق والعلوم الإنسانية. العدد، 03، 2020. ص 174 -175

[3] . مسوس، كمال. حديد، نوفل. **مقاربة حماية أنظمة معلومات المؤسسة من الاعتداءات الالكترونية**. مجلة المؤسسة. المجلد، 05. العدد، 05، 2016. ص 37- 38

[4]. حزام، فتيحة. **المرجع السابق**. ص 177

وفي نفس الصدد نجد ان وسائل حماية الانترنيت انتقلت من مستويات الحماية الفردية التي تقوم على وضع وسائل الحماية ومنها الجدران النارية في المؤسسة، الى مستويات الامن المتعددة والتي تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع من المعلومات أو نظم المعلومات داخل الشبكة الخاصة، وتعتمد وسائل الامن متعددة الاتجاهات والاغراض اليات مختلفة لتوفير الأمن الشامل للنظام Comprehensive Security System وتتضمن ثلاثة مناطق أساسية وهي:[1]

- ✓ إدارة خطوات الأمن وتشمل الخطط والاستراتيجيات وأغراضها وكذلك المنتجات وقواعد الانتاج والبحث والتحليل.
- ✓ أنواع الحماية وتشمل الوقاية أو الحماية والتحقق والتحري والتصرف.
- ✓ وسائل الحماية وتشمل حماية النظم والخوادم وحماية البنية التحتية للشبكة.

2. أنظمة كشف التسلل IDS وأنظمة منع التسللIPS:

تعد أنظمة كشف ومنع التسلل (Intrusion Detection and Prevention System) أهم الأدوات الأمنية المستخدمة في المكتبات الجامعية لحماية البنية التحتية الرقمية من التهديدات السيبرانية. تعمل أنظمة كشف التسلل (IDS) على مراقبة الشبكة وتحليل حركة البيانات لاكتشاف أي نشاط مشبوه أو محاولات اختراق، بينما تقوم أنظمة منع التسلل (IPS) باتخاذ إجراءات تلقائية لمنع هذه التهديدات قبل أن تلحق ضررًا بالأنظمة. تعتمد هذه الأنظمة على تقنيات الذكاء الاصطناعي والتعلم الآلي لتحليل السلوكيات غير الطبيعية للمستخدمين، مما يساعد في التعرف على الهجمات السيبرانية مثل محاولات الدخول غير المصرح بها، وهجمات رفض الخدمة (DDoS)، والبرمجيات الضارة. بفضل هذه التقنيات، تتمكن المكتبات الجامعية من تأمين بياناتها الرقمية، وحماية مواردها الإلكترونية، وضمان استمرارية خدماتها دون انقطاع، مما يعزز من أمان البيئة الأكاديمية الرقمية. [2]

أ. نظام منع التسللIPS: هو أحد أبرز الحلول الأمنية المستخدمة لحماية الشبكات والأنظمة الرقمية من الهجمات السيبرانية. يعمل هذا النظام على مراقبة حركة البيانات داخل الشبكة بشكل مستمر، وتحليلها

---

[1] . نجاري بن حاح علي. فايزة. **جريمة التجسس الالكتروني**. مجلة دراسات الدفاع والاسقبالية. المجلد، 01. العدد، 11، 2019. ص 69

[2] .عادل نبيل، شحات علي. **تقنيات أمن وحماية المعلومات الرقمي للمستودع الرقمي للرسائل الجامعية المصرية**. مجلة كلية الآداب. المجلد، 01. العدد، 48، 2017. ص 75

لاكتشاف أي نشاط مشبوه أو محاولات اختراق، ومن ثم اتخاذ إجراءات فورية لمنع التهديدات قبل أن تسبب أي ضرر. يعتمد IPS على تقنيات متقدمة مثل: [1]

- تحليل التوقيعات (Signature-BasedDetection)
- تحليل السلوك غير الطبيعي (Behavior-BasedDetection)
- الكشف عن الشذوذ في البروتوكولات (Protocol AnomalyDetection)

مما يمكنه من التعرف بدقة على الهجمات السيبرانية المختلفة مثل:[2]

- هجمات الفدية (Ransomware)
- هجمات القوة الغاشمة (Brute Force Attacks)
- هجمات رفض الخدمة (DDoS)
- البرمجيات الضارة (Malware)

يعمل نظام IPS من خلال عدة مراحل متكاملة، تبدأ برصد وتحليل حركة البيانات داخل الشبكة، ثم تحديد أي تهديدات محتملة، وأخيرًا اتخاذ الإجراءات المناسبة لمواجهتها. عند اكتشاف أي نشاط ضار، يقوم النظام بتنفيذ أحد الإجراءات التالية:[3]

- ✓ حظر عنوان IP الخاص بالمهاجم لمنعه من الوصول إلى الشبكة مجددًا.
- ✓ إيقاف الجلسات غير المصرح بها والتي قد تستخدم لاختراق النظام.
- ✓ منع تشغيل الأكواد الضارة التي قد تستهدف الأجهزة أو الخوادم داخل المكتبة.
- ✓ إرسال تنبيهات فورية إلى فرق الأمن السيبراني لاتخاذ إجراءات إضافية عند الحاجة.
- ✓ تحديث قواعد البيانات الأمنية تلقائيًا لضمان التصدي للتهديدات المشابهة في المستقبل.

تلعب المكتبات الجامعية دورًا أساسيًا في دعم العملية التعليمية والبحثية من خلال توفير أنظمة رقمية متطورة، وقواعد بيانات أكاديمية، وخدمات إلكترونية تتيح للطلاب والأساتذة الوصول إلى المعلومات بسهولة.

---

[1] . عادل نبيل، شحات علي. **المرجع نفسه**. ص 77

[2] . عادل نبيل، شحات علي. **المرجع السابق**. ص 78

[3]. International protective service. **IPS Security**. Visit: 13/03/2025. 16 :34. Constable on https://ip.global.com

ومع تزايد الاعتماد على التقنيات الرقمية، أصبح من الضروري حماية هذه المكتبات من التهديدات السيبرانية التي قد تؤدي إلى اختراق البيانات، أو تعطيل الخدمات، أو إتلاف المعلومات المخزنة. في هذا السياق، يعد نظام منع التسلل Intrusion Prevention System، أحد الحلول الأمنية الفعالة التي تساهم في تعزيز الحماية الرقمية للمكتبات الجامعية.

فيما يلي تفصيل لأهميته:[1]

- منع الهجمات السيبرانية قبل وقوعها: بخلاف نظام كشف التسلل (IDS)، الذي يكتفي برصد التهديدات وتحذير فرق الأمن السيبراني، يعمل IPS على إيقاف الهجمات بشكل تلقائي وفوري قبل أن تسبب أي ضرر. يمكنه التصدي لمجموعة متنوعة من الهجمات، مثل:

✓ هجمات الفدية (Ransomware Attacks)، التي تحاول تشفير بيانات المكتبة وطلب فدية لفك التشفير.

✓ هجمات القوة الغاشمة (Brute Force Attacks)، التي تستهدف اختراق حسابات المستخدمين عبر تجريب عدد كبير من كلمات المرور.

✓ هجمات رفض الخدمة (DDoS Attacks)، التي تهدف إلى تعطيل أنظمة المكتبة عبر إرسال كميات هائلة من الطلبات.

- حماية قواعد البيانات الأكاديمية والمعلومات الحساسة: تحتوي المكتبات الجامعية على كم هائل من الأبحاث العلمية، والدراسات الأكاديمية، وبيانات المستخدمين، مما يجعلها هدفًا جذابًا للقراصنة. حيث يعمل IPS على مراقبة حركة البيانات بين الأجهزة والخوادم، وحظر أي محاولات غير مصرح بها للوصول إلى البيانات الحساسة، مما يمنع التلاعب أو تسريب المعلومات.

- تعزيز استمرارية الخدمات الإلكترونية للمكتبات: تعتمد المكتبات الحديثة على أنظمة إلكترونية متكاملة لإدارة عمليات البحث، والاستعارة، والخدمات الأكاديمية عبر الإنترنت. ويساهم IPS في ضمان استمرارية هذه الخدمات دون انقطاع عبر التصدي للهجمات التي قد تتسبب في تعطل الخوادم أو شلل الأنظمة الرقمية.على سبيل المثال، إذا حاول أحد القراصنة تنفيذ هجوم رفض الخدمة (DDoS)، يقوم IPS بتحليل حركة البيانات وحظر العناوين المشبوهة فورًا لمنع توقف خدمات المكتبة.

---

[1]. Ben abdallâh, Ahceneyoucef. Boudour, Rachid. **Approche complète de développement des IPS pour les socs**. Synthes. Volume. 22, Numero,01, 2016. P 05- 07

- تأمين حسابات الطلاب والباحثين وحماية بيانات تسجيل الدخول: يستخدم الطلاب وأعضاء هيئة التدريس حسابات رقمية للوصول إلى موارد المكتبة، مما يجعلها عرضة لهجمات التصيد الإلكتروني وسرقة بيانات تسجيل الدخول. فيقوم IPS بمنع محاولات تسجيل الدخول المشبوهة عبر تقنيات مثل:[1]

✓ تحليل سلوك المستخدمين لاكتشاف المحاولات غير الطبيعية.

✓ حظر العناوين المشبوهة التي تحاول الوصول إلى الحسابات بطرق غير قانونية.

✓ إيقاف الهجمات التي تستهدف استغلال الثغرات الأمنية في أنظمة المصادقة الخاصة بالمكتبة.

- تحسين استجابة فرق الأمن السيبراني داخل الجامعات: يوفر IPS تقارير وتحليلات تفصيلية عن التهديدات الأمنية التي تم التصدي لها، مما يساعد فرق الأمن السيبراني على:[2]

✓ تحليل أنماط الهجمات وتحديد المصادر المحتملة للتهديدات.

✓ اتخاذ قرارات أمنية استباقية لمنع وقوع هجمات مستقبلية.

✓ تعزيز بروتوكولات الأمان وتحسين سياسات الحماية داخل المكتبة.

- الامتثال للمعايير الأمنية وحماية السمعة الأكاديمية: تلتزم الجامعات بمعايير أمنية عالمية مثل ISO 27001 لحماية البيانات، ويعد استخدام IPS جزءًا أساسيًا من تحقيق الامتثال لهذه المعايير، ويساعد في حماية سمعة المكتبة الجامعية، حيث إن أي اختراق أمني قد يؤدي إلى فقدان ثقة الطلاب والباحثين في الخدمات الإلكترونية. [3]

ب. نظام كشف التسلل Intrusion Detection System

يعتبر من الأدوات الأمنية الأساسية التي تُستخدم لمراقبة الشبكات والأنظمة الرقمية واكتشاف أي أنشطة مشبوهة أو محاولات اختراق. يتمثل دوره الرئيسي في تحليل حركة البيانات داخل الشبكة ورصد أي سلوك غير طبيعي، مما يساعد في الكشف المبكر عن الهجمات السيبرانية مثل محاولات الاختراق، والبرمجيات الضارة، وهجمات رفض الخدمة (DDoS)، وهجمات القوة الغاشمة (Brute Force Attacks). بخلاف نظام منع التسلل (IPS)، لا يقوم IDS باتخاذ إجراءات وقائية بشكل تلقائي، لكنه يوفر تنبيهات وتحذيرات إلى فرق

---

[1]. Abdallah Abdelkarim, Amjad. **Intrusion prevention system**. International journal of Academic Research. Vol,03. No,01, 2011.P 432

[2]. Abdallah Abdelkarim, Amjad. **Ibid**. P 433

[3]. عادل نبيل، شحات علي. **المرجع السابق**. ص 81

الأمن السيبراني حتى يتمكنوا من التدخل بسرعة ومعالجة التهديدات قبل أن تتفاقم.[1] ويعتمد نظام كشف التسلل على تقنيات تحليل متقدمة للكشف عن التهديدات، ويعمل بإحدى الطريقتين الرئيسيتين:

- الكشف المعتمد على التوقيعات (Signature-BasedDetection): يقارن IDS حركة البيانات مع قاعدة بيانات تحتوي على أنماط معروفة للهجمات الإلكترونية. إذا تم اكتشاف تطابق، يتم إرسال تنبيه أمني إلى فرق الأمن السيبراني.
- الكشف القائم على السلوك (Anomaly-BasedDetection): يراقب IDS سلوك المستخدمين والأنظمة بشكل مستمر، وإذا لاحظ أي نشاط غير عادي أو غير متوقع، مثل عدد محاولات تسجيل دخول متكررة بشكل غير طبيعي، فإنه يقوم بتنبيه المسؤولين لاتخاذ الإجراء المناسب.

حيث تلعب المكتبات الجامعية دورًا محوريًا في تقديم الخدمات الأكاديمية والبحثية، حيث توفر بيئة رقمية غنية بالموارد والمعلومات للطلاب والباحثين. ومع تزايد الاعتماد على الأنظمة الرقمية وقواعد البيانات الإلكترونية، أصبحت المكتبات هدفًا محتملاً للهجمات السيبرانية التي قد تؤدي إلى سرقة البيانات، وتعطيل الخدمات، والتلاعب بالمعلومات الأكاديمية. في هذا السياق، ويُعد نظام كشف التسلل (IDS) أداة أساسية لتعزيز الأمن السيبراني داخل المكتبات الجامعية، وذلك من خلال:

- ✓ حماية قواعد البيانات الأكاديمية والمحتوى الرقمي: تحتوي المكتبات الجامعية على كم هائل من الأبحاث العلمية، والكتب الإلكترونية، والأطروحات الجامعية التي تعتبر ذات قيمة كبيرة للمؤسسات التعليمية والباحثين. ويساهم IDS في حماية هذه البيانات من الاختراق أو التلاعب من خلال مراقبة الأنشطة غير الطبيعية واكتشاف أي محاولات وصول غير مصرح بها.
- ✓ منع سرقة بيانات المستخدمين وتأمين الحسابات: يستخدم الطلاب والأساتذة أنظمة المكتبة الإلكترونية من خلال حسابات تسجيل الدخول، والتي قد تكون عرضة لهجمات التصيد الإلكتروني (Phishing)، أو هجمات القوة الغاشمة (Brute Force Attacks). ويساهم IDS في رصد المحاولات المتكررة لاختراق الحسابات، ويقوم بتنبيه فرق الأمن لاتخاذ الإجراءات الوقائية مثل إعادة تعيين كلمات المرور أو حظر العناوين المشبوهة[2].
- ✓ منع سرقة بيانات المستخدمين وتأمين الحسابات: يستخدم الطلاب والأساتذة أنظمة المكتبة الإلكترونية من خلال حسابات تسجيل الدخول، والتي قد تكون عرضة لهجمات التصيد الإلكتروني (Phishing)، أو

---

[1]. Abdallah Abdelkarim, Amjad. **Ibid**. P 433

[2]. Abdallah Abdelkarim, Amjad. **Ibid**. P 433

هجمات القوة الغاشمة (Brute Force Attacks). ويساهم IDS في رصد المحاولات المتكررة لاختراق الحسابات، ويقوم بتنبيه فرق الأمن لاتخاذ الإجراءات الوقائية مثل إعادة تعيين كلمات المرور أو حظر العناوين المشبوهة.

- ✓ ضمان استمرارية الخدمات الرقمية للمكتبات: تعتمد المكتبات الحديثة على أنظمة البحث الإلكتروني، وأنظمة الاستعارة الرقمية، والخدمات السحابية، مما يجعلها عرضة لهجمات تعطيل الخدمة (DDoS). يعمل IDS على رصد أي ارتفاع غير طبيعي في حركة البيانات، مما يساعد في التصدي لهذه الهجمات قبل أن تؤدي إلى تعطيل الأنظمة وإيقاف الخدمات.
- ✓ تحسين استجابة فرق الأمن السيبراني: يوفر IDS بيانات تفصيلية حول التهديدات والهجمات المحتملة، مما يساعد فرق الأمن السيبراني في تحليل نقاط الضعف داخل الشبكة واتخاذ إجراءات استباقية لتعزيز الدفاعات الأمنية. بالإضافة إلى ذلك، فهو يساهم في تحديد الثغرات الأمنية في الأنظمة، مما يساعد على تطوير سياسات أمنية أكثر كفاءة لحماية المكتبة من الهجمات المستقبلية[1].
- ✓ تعزيز ثقة الطلاب والباحثين في أمن الأنظمة الإلكترونية: عندما يشعر المستخدمون بأن أنظمة المكتبة الإلكترونية مؤمنة جيدًا، فإنهم يكونون أكثر راحة في استخدامها دون الخوف من سرقة بياناتهم أو فقدان أبحاثهم. يساهم IDS في بناء هذه الثقة من خلال توفير بيئة رقمية آمنة ومستقرة، مما يعزز استخدام الموارد الإلكترونية بشكل فعال داخل المؤسسات الأكاديمية.
- ✓ دعم الامتثال للمعايير والسياسات الأمنية: تحتاج المؤسسات الأكاديمية إلى الالتزام بالمعايير الأمنية الدولية لحماية بياناتها، مثل معايير الأمان في الشبكات (ISO/IEC 27001) وقوانين حماية البيانات. يساعد IDS في ضمان الامتثال لهذه السياسات من خلال مراقبة الامتثال الأمني، واكتشاف أي تجاوزات، والتأكد من تنفيذ بروتوكولات الحماية اللازمة.

❖ أنظمة التشفير (Encryptions systemes):

تلعب أنظمة التشفير دورًا حيويًا في حماية الشبكات وتأمين البيانات داخل المكتبات الجامعية، حيث تعمل على تحويل البيانات إلى صيغة غير مقروءة إلا للأشخاص المخوّلين بفك تشفيرها. تعتمد هذه الأنظمة على خوارزميات رياضية معقدة مثل AES/RSA لضمان سرية المعلومات أثناء تخزينها أو نقلها عبر الشبكات. في سياق المكتبات الجامعية، تساهم أنظمة التشفير في حماية بيانات الطلاب والباحثين، وتأمين قواعد البيانات الرقمية، وضمان سرية الاتصالات بين المستخدمين وخوادم المكتبة. على سبيل المثال، عند دخول المستخدم إلى مكتبة رقمية عبر الإنترنت، يتم استخدام بروتوكولات تشفير مثل SSL/TLS لضمان أن الاتصال آمن وأن بيانات

[1]. Abdallah Abdelkarim, Amjad. **Ibid**. P 433

تسجيل الدخول غير معرضة للاختراق. بالإضافة إلى ذلك، تساعد أنظمة التشفير في منع الوصول غير المصرح به إلى الموارد الأكاديمية المخزنة على الخوادم، حيث يتم تشفير الملفات الرقمية مثل الكتب الإلكترونية والمقالات البحثية، مما يضمن أن الوصول إليها يقتصر على المستخدمين المصرح لهم فقط.[1]

كما يلعب هذا النظام دورًا أساسيًا في مكافحة الهجمات السيبرانية مثل: التصيد الاحتيالي والتجسس الإلكتروني، حيث تجعل البيانات عديمة الفائدة للقراصنة حتى في حالة اعتراضها أثناء نقلها عبر الشبكة. علاوة على ذلك، ترتبط أنظمة التشفير ارتباطًا وثيقًا بأمن المعلومات في المكتبات الجامعية من خلال تعزيز أهم المبادئ والتي تتمثل في:[2]

- مبدأ السرية (Confidentiality).
- مبدأ السلامة (Integrity).
- مبدأ التوفر (Availability).

مما يضمن بيئة بحثية آمنة تحافظ على خصوصية المستخدمين وتحمي الأصول المعلوماتية القيمة للمكتبة. ومن هنا، فإن الاستثمار في تقنيات التشفير الحديثة يعد ضرورة حتمية لمواكبة التهديدات السيبرانية المتزايدة في المجال الأكاديمي. ويتمثل دور نظام التشفير فيما يلي: [3]

1. حماية بيانات المستخدمين وضمان الخصوصية: تعد حماية بيانات المستخدمين من أهم أدوار أنظمة التشفير في المكتبات الجامعية، حيث تتضمن المكتبات الإلكترونية معلومات حساسة مثل بيانات تسجيل الدخول، والسجلات الأكاديمية، وتاريخ البحث والاستعارة. من خلال تطبيق تشفير البيانات المخزنة، يتم تحويل هذه المعلومات إلى صيغة غير مقروءة إلا من قبل المستخدمين المخوّلين، مما يمنع الوصول غير المصرح به حتى في حالة تعرض قاعدة البيانات للاختراق. كما تساهم بروتوكولات مثل SSL/TLS في حماية جلسات المستخدمين أثناء تصفح المكتبة الرقمية، مما يمنع المهاجمين من اعتراض بيانات الاتصال وسرقتها.
2. تأمين نقل البيانات عبر الشبكات: تعتمد المكتبات الجامعية على الشبكات المحلية (LAN) أو الإنترنت لتوفير الوصول إلى مواردها الرقمية، مما يجعلها عرضة لهجمات التنصت والاختراقات. وهنا يأتي دور تشفير

---

[1] . داودي، منصور. مرابط، حمزة. **التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية**. مجلة الحقوق والعلوم السياسية. المجلد، 10. العدد،01، 2023. ص 30

[2] . داودي، منصور. مرابط، حمزة. **المرجع السابق**. ص 32

[3]. غريبي، أحمد. قاسيمي، حورية. **دور سياسة التشفير الاليكتروني في حماية نظم معلومات الإدارة الالكترونية**. مجلة الاقتصاد الجديد. المجلد، 12. العدد، 01، 2021. ص 310 -311

البيانات أثناء النقل حيث يتم استخدام بروتوكولات مثل: IP Sec HTTPS/VPN لضمان أن جميع الاتصالات بين أجهزة المستخدمين وخوادم المكتبة تكون مشفرة وآمنة. على سبيل المثال: عند قيام الباحث بتنزيل ورقة بحثية[1].

يتم تشفير الاتصال لضمان أن البيانات لا يمكن اعتراضها أو تعديلها من قبل أطراف غير مخوّلة.

3. منع التلاعب بالبيانات وضمان سلامتها: تلعب أنظمة التشفير دورًا مهمًا في ضمان سلامة البيانات (Data Integrity) داخل المكتبات الجامعية، حيث يمكن للمهاجمين التلاعب بالمحتوى الرقمي، أو تعديل المعلومات المخزنة، أو حذفها دون إذن. باستخدام تقنيات التوقيع الرقمي (Digital Signatures) والتشفير بالمفتاح العام (Public Key Cryptography)، يتم التأكد من أن أي تعديل غير مصرح به في البيانات سيتم اكتشافه فورًا. على سبيل المثال: عند مشاركة ملفات إلكترونية بين أعضاء هيئة التدريس والطلاب، يتم تطبيق تقنيات التحقق من الهوية والتشفير لضمان أن المحتوى لم يتم العبث به أثناء النقل.[2]

4. تعزيز الحماية ضد الهجمات السيبرانية: تتعرض المكتبات الجامعية لمحاولات اختراق إلكتروني وهجمات خبيثة تستهدف بيانات المستخدمين أو تعطل الخدمات الرقمية. تلعب أنظمة التشفير دورًا أساسيًا في حماية المكتبات من هذه الهجمات من خلال:

- التصدي لهجمات سرقة الهوية (Identity Theft): عبر استخدام تقنيات المصادقة القوية مثل: التشفير ثنائي المفتاح (Asymmetric Encryptions)، مما يجعل من الصعب على المهاجمين انتحال هوية المستخدمين.
- منع هجمات القراصنة: التي تحدث عندما يعترض القراصنة الاتصالات بين المستخدمين وخوادم المكتبة، حيث يتم حماية البيانات عبر بروتوكولات تشفير قوية تجعل اعتراضها عديم الفائدة.
- حماية المكتبة من هجمات الفدية (Ransomware): عبر تشفير البيانات الاحتياطية بحيث لا يمكن للمهاجمين تشفيرها وطلب فدية لاسترجاعها.[3]

5. دعم إدارة الهوية والصلاحيات: تساعد أنظمة التشفير في إدارة الهوية والتحكم في الصلاحيات (Identity and Access Management – IAM) داخل المكتبات الجامعية، حيث يتم تحديد من يمكنه

---

[1] . غريبي، أحمد. قاسيمي، حورية. **المرجع نفسه**. 313

[2] . غريبي، أحمد. قاسيمي، حورية. **المرجع السابق**. 313

[3] . بورابة، صورية. **قواعد الأمن المعلوماتي**. أطروحة لنيل شهادة الدكتوراه. كلية الحقوق والعلوم الإنسانية. قسم الحقوق: تخصص قانون خاص. جامعة جيلالي اليابس. سيدي بلعباس، 2016

الوصول إلى الموارد الرقمية، ومن يمكنه إجراء تعديلات على قاعدة البيانات، ومن لديه صلاحية التحميل أو التعديل. باستخدام التشفير القائم على الأدوار، يتم منح كل مستخدم مفاتيح تشفير محددة تسمح له فقط بالوصول إلى البيانات المصرح بها، مما يمنع التلاعب الداخلي أو إساءة استخدام البيانات من قبل الموظفين أو المستخدمين غير المخوّلين.[1]

6. تعزيز الثقة في الخدمات الإلكترونية للمكتبة: عندما يشعر الطلاب والباحثون بأن بياناتهم الشخصية والمعلومات الأكاديمية محمية جيدًا داخل المكتبة الجامعية، فإن ذلك يعزز من ثقتهم في استخدام الخدمات الإلكترونية مثل البحث في قواعد البيانات، وتنزيل الكتب الرقمية، والمشاركة في المناقشات الأكاديمية عبر الإنترنت. تساهم أنظمة التشفير في ضمان مصداقية المكتبة الجامعية كمنصة آمنة للبحث العلمي، وتشجع المزيد من الطلاب وأعضاء هيئة التدريس على الاستفادة من مواردها الرقمية.[2]
7. دعم تقنيات النسخ الاحتياطي الآمن واستعادة البيانات: تساعد أنظمة التشفير المكتبات الجامعية في إدارة النسخ الاحتياطي للبيانات بطرق آمنة، حيث يتم تشفير النسخ الاحتياطية المخزنة محليًا أو في السحابة لمنع الوصول غير المصرح به إليها. في حالة تعرض المكتبة لهجوم سيبراني أو عطل تقني، يمكن استعادة البيانات بسهولة دون القلق من سرقتها أو التلاعب بها، مما يضمن استمرارية الخدمات الرقمية دون انقطاع.[3]

❖ أنظمة إدارة الهوية والصلاحيات IAM:

تُعد أنظمة إدارة الهوية والصلاحيات Identity and Access Management، من الحلول الأساسية في تعزيز الأمن السيبراني في المؤسسات المختلفة، بما في ذلك المكتبات الجامعية. وتعمل هذه الأنظمة على إدارة والتحكم في هوية المستخدمين، وتحديد الصلاحيات المسموح بها، وضمان وصول الأشخاص المخولين فقط إلى الموارد الرقمية والخدمات الإلكترونية. تعتمد أنظمة IAM على مجموعة من العمليات والتقنيات التي تضمن أن المستخدمين المصرح لهم فقط يمكنهم الوصول إلى البيانات والأنظمة الرقمية. وتشمل هذه العمليات:

✓ إدارة الهويات (Identity Management): وهي عملية إنشاء وإدارة هويات المستخدمين داخل النظام، مثل الطلاب، أعضاء هيئة التدريس، والموظفين الإداريين.

---

[1] . بوربابة، صورية. **المرجع نفسه**. ص 50

[2] . نقموش، عادل. **حوكمة المؤسسات ودورها في تحقيق جودة المعلومات المحاسبية**. مجلة البحث الاقتصاد الإداري. المجلد، 16. العدد، 02، 2022. ص 65

[3] . نقموش، عادل. **المرجع نفسه**. ص 66

- ✓ إدارة الوصول (Access Control): وهي تحديد الصلاحيات الممنوحة لكل مستخدم وفقًا لدوره الوظيفي، مثل الوصول إلى قواعد البيانات أو تحميل الكتب الإلكترونية[1].
- ✓ التوثيق والتحقق من الهوية (Authentication et Autorisation): باستخدام كلمات المرور، والتسجيل الثنائي (FA2)، وتقنيات التعرف البيو متري لضمان أمان تسجيل الدخول.

وتلعب أنظمة إدارة الهوية والصلاحيات (IAM) دورًا محوريًا في تعزيز الأمن السيبراني داخل المكتبات الجامعية، حيث تضمن وصول المستخدمين المصرح لهم فقط إلى الموارد والخدمات الرقمية، مما يحمي المعلومات الأكاديمية الحساسة من الاختراقات وسوء الاستخدام. من خلال تحديد صلاحيات الوصول بدقة، تمنع IAM الوصول غير المصرح به إلى قواعد البيانات، والأبحاث العلمية، والمحتوى الرقمي، مما يقلل من مخاطر التسلل السيبراني وهجمات سرقة الهوية. إضافة إلى ذلك، تسهم IAM في تحسين تجربة المستخدم عبر توفير أنظمة مصادقة موحدة (SSO) تتيح للطلاب وأعضاء هيئة التدريس الوصول بسهولة وأمان إلى جميع الخدمات الإلكترونية بحساب واحد، دون الحاجة إلى إدخال بيانات تسجيل الدخول بشكل متكرر. كما تساعد في الامتثال للمعايير الأمنية مثل: قانون حماية البيانات (GDPR)، من خلال فرض سياسات وصول صارمة ومراقبة الأنشطة المشبوهة عبر سجلات التدقيق (Audit Logs). علاوة على ذلك، تعمل IAM على تقليل العبء الإداري عبر إدارة الحسابات تلقائيًا، مثل تعطيل حسابات الطلاب بعد التخرج أو تحديث صلاحيات الموظفين عند تغير مناصبهم. بفضل هذه الميزات، تعد IAM حجر الأساس للأمن السيبراني في المكتبات الجامعية، حيث تضمن بيئة رقمية آمنة ومستدامة تدعم البحث الأكاديمي والتعلم الإلكتروني بشكل موثوق.[2]

❖ الذكاء الاصطناعي وتحليل البيانات في الأمن السيبيراني:

يعد الذكاء الاصطناعي (AI) وتحليل البيانات الضخمة من الأدوات الحديثة والفعالة في تعزيز الأمن السيبراني داخل المكتبات الجامعية، حيث توفر تقنيات مثل: التعلم الآلي (Machine Learning) وتحليل السلوك السيبراني (Behavioral Analytics) القدرة متقدمة على اكتشاف التهديدات الأمنية والاستجابة لها بذكاء وسرعة. بحيث نجد أنظمة التعلم الآلي تعمل على تحليل كميات ضخمة من البيانات وتحديد الأنماط

---

[1]. National Cybersecurity centre of Excellence. **Identity and Access Management (IAM) Cyber security**. Visit: 14/03/2025. 15:23. Constable on: https://www.nccoe.nist.gov

[2]. National Cybersecurity centre of Excellence. **Identity and Access Management (IAM) Cyber security**. Visit: 14/03/2025. 15:23. Constable on: https://www.nccoe.nist.gov

الشاذة التي قد تشير إلى محاولات اختراق أو أنشطة غير مشروعة، مثل الوصول غير المصرح به إلى قواعد البيانات[1].

أو محاولات سرقة المعلومات الأكاديمية. كما تساهم أنظمة التحليل السلوكي في مراقبة سلوك المستخدمين داخل الشبكات، مما يمكنها من التنبؤ بالهجمات السيبرانية قبل وقوعها، وذلك من خلال رصد أي تغييرات مفاجئة أو غير معتادة في أنماط تسجيل الدخول أو عمليات تنزيل الملفات.[2]

في المكتبات الجامعية، يساعد الذكاء الاصطناعي في حماية البنية التحتية الرقمية عبر الكشف التلقائي عن البرمجيات الخبيثة، وإيقاف الهجمات السيبرانية مثل التصيد الاحتيالي (Phishing) وهجمات الفدية (Ransomware). كما تسهم هذه التقنيات في تحليل بيانات المستخدمين بشكل آمن، مما يسمح بتطوير استراتيجيات دفاعية مخصصة لضمان استمرارية الخدمات الرقمية دون تعطل. وبفضل قدراتها على التعلم والتكيف، تتيح أنظمة الذكاء الاصطناعي تحليل البيانات في الوقت الفعلي، مما يجعلها أداة حيوية لتعزيز الحماية الإلكترونية وضمان بيئة رقمية آمنة ومستدامة في المكتبات الجامعية.

أ. يُعد التعلم الآلي (Machine Learning): من أهم تقنيات الذكاء الاصطناعي المستخدمة في تعزيز الأمن السيبراني، حيث يمكنه تحليل البيانات الضخمة، اكتشاف التهديدات السيبرانية في الوقت الفعلي، والتنبؤ بالهجمات المستقبلية من خلال التعلم من الأنماط السابقة. في المكتبات الجامعية، التي تعتمد على الأنظمة الرقمية لإدارة البيانات الأكاديمية والخدمات الإلكترونية، تساهم تقنيات التعلم الآلي في حماية قواعد البيانات، تأمين أنظمة المصادقة، ورصد الأنشطة المشبوهة لمنع الاختراقات والتهديدات الإلكترونية. حيث تعتمد تقنيات التعلم الآلي على تحليل كميات هائلة من البيانات، ثم بناء نماذج قادرة على التعرف على الأنماط الطبيعية للسلوك الإلكتروني، مما يساعد في اكتشاف أي سلوك غير طبيعي قد يشير إلى تهديد أمني. وتنقسم خوارزميات التعلم الآلي المستخدمة في الأمن السيبراني إلى عدة أنواع منها:

- التعلم المراقب (Supervised Learning): يتم تدريب النموذج باستخدام بيانات مصنفة مسبقًا تحتوي على أمثلة للأنشطة الطبيعية والمشبوهة، مما يساعد النظام على التعرف بدقة على الهجمات المحتملة مثل محاولات تسجيل الدخول غير المشروعة في أنظمة المكتبات.

---

[1] . بن مهيدي، مرزوق. سعيدي، خليل. **الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبيراني**. مجلة السلام للعلوم الإنسانية والاجتماعية. المجلد، 06. العدد، 01، 2022. ص 26 -28

[2] . بن مهيدي، مرزوق. سعيدي، خليل. **الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبيراني**. مجلة السلام للعلوم الإنسانية والاجتماعية. المجلد، 06. العدد، 01، 2022. ص 26 -28

- التعلم غير المراقب (Unsupervised Learning): يعتمد على تحليل البيانات دون الحاجة إلى تصنيف مسبق، مما يجعله فعالًا في اكتشاف الهجمات السيبرانيةالجديدة من خلال تحديد الأنشطة غير العادية التي تختلف عن السلوك المعتاد للمستخدمين[1].
- التعلم المعزز (Renforcement Learning): يعتمد على تحسين أداء النظام بشكل مستمر من خلال التفاعل مع البيئة الإلكترونية، مما يساعد في تحسين استراتيجيات الحماية وتطوير أنظمة دفاع سيبراني أكثر ذكاءً.

ب. أنظمة التحليل السلوكي (Behavioral Analytics Systems): هي تقنيات متقدمة تُستخدم في رصد وتحليل سلوك المستخدمين والأنظمة للكشف عن الأنشطة غير الطبيعية أو المشبوهة التي قد تشير إلى محاولات اختراق أو تهديدات أمنية. تعتمد هذه الأنظمة على الذكاء الاصطناعي والتعلم الآلي لتحليل البيانات الكبيرة وتحديد الأنماط السلوكية المعتادة، ومن ثم اكتشاف أي انحرافات قد تدل على هجومات سيبرانية. وتكمن أهمية هذا النظام فيما يلي: [2]

- ✓ الكشف عن التهديدات غير المعروفة: على عكس أنظمة الحماية التقليدية التي تعتمد على قواعد ثابتة، تستطيع أنظمة التحليل السلوكي اكتشاف الهجمات الجديدة التي لم يتم توثيقها مسبقًا.
- ✓ منع الاختراقات الداخلية: يمكنها التعرف على السلوكيات المشبوهة حتى لو صدرت من مستخدمين موثوق بهم داخل المؤسسة، مثل موظف يحاول تسريب بيانات حساسة.
- ✓ التصدي لهجمات الهندسة الاجتماعية والتصيد الاحتيالي: تستطيع الأنظمة اكتشاف محاولات الدخول غير الطبيعية الناتجة عن اختراق حسابات المستخدمين.
- ✓ تحليل البيانات الضخمة في الوقت الفعلي: مما يساعد على اتخاذ قرارات أمنية سريعة وفعال

وبالتالي فان التكامل الفعال بين السياسات الأمنية والتقنيات الحديثة يؤدي إلى تحسين جودة الخدمات التي تقدمها المكتبات الجامعية، ومن أبرز هذه التأثيرات الإيجابية التي يمكن طرحها هي:

---

[1] . بن برغوث، ليلى. **الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي**. المجلة الدولية لاتصال الاجتماعي. المجلد، 10. العدد، 01، 2023. ص 446

[2] . لعجال، حمزة. موفق، عبد المالك. **التقنيات الحديثة في المكتبات الجامعية الداعمة لذوي الاحتياجات الخاصة: دراسة لنماذج وإمكانية اعتمادها في المكتبات الجامعية بجامعة مسيلة**. مجلة ببيوغرافيا لدراسات المكتبات والمعلومات. المجلد، 01. العدد، 01، 2019. ص 110- 112

- ✓ تعزيز استمرارية الخدمات الرقمية: يضمن الأمن السيبراني الفعال حماية الأنظمة من التوقف بسبب الهجمات الإلكترونية، مما يحافظ على استمرارية الخدمات مثل قواعد البيانات الرقمية والمكتبات الإلكترونية[1].

تمكن خطط الطوارئ واستراتيجيات النسخ الاحتياطي من استعادة البيانات بسرعة بعد أي عطل مفاجئ.

- ✓ تحسين تجربة المستخدمين: توفر المكتبات بيئة بحث آمنة وسريعة بفضل الخوادم المحمية وتقنيات التشفير، ويمكن للطلاب والباحثين الوصول إلى الموارد بسهولة دون القلق بشأن سرقة بياناتهم أو التعرض للاختراقات.[2]

- ✓ تقليل التهديدات الداخلية والخارجية: تمنع السياسات الأمنية والتقنيات الحديثة التسريبات الداخلية عبر تقييد صلاحيات الموظفين والمستخدمين. وتكشف أنظمة الذكاء الاصطناعي الأنشطة غير الطبيعية وتتصدى لها تلقائيًا [3].

- ✓ تحسين إدارة البيانات والموارد: تتيح التقنيات الحديثة تنظيم وفهرسة البيانات بشكل أكثر كفاءة، مما يسهل عمليات البحث والاسترجاع. بالإضافة ال أن تساعد أنظمة إدارة المكتبات (LMS) في تتبع استعارات الكتب وإدارة الحسابات الرقمية للمستخدمين بفعالية.[4]

- ✓ تعزيز الثقة في الخدمات المكتبية: يشعر المستخدمون بمزيد من الأمان عند استخدام المكتبات الرقمية، مما يزيد من الإقبال على الاستفادة من الموارد الأكاديمية المتاحة، بالإضافة ال يمنح الامتثال للمعايير الأمنية المكتبة سمعة قوية ويعزز تعاونها مع مؤسسات بحثية أخرى.

- ✓ تحسين كفاءة الخدمات الرقمية: تؤدي الحوكمة إلى تحسين كفاءة أنظمة البحث الرقمي، مما يسهل الوصول إلى الموارد الأكاديمية بسرعة وأمان. وتعمل على تقليل زمن تعطل الأنظمة الرقمية، مما يضمن استمرارية الخدمات المقدمة للطلاب والباحثين.[5]

---

[1] . لعجال، حمزة. موفق، عبد المالك. **المرجع نفسه**. ص 114

[2] . لعجال، حمزة. موفق، عبد المالك. **المرجع السابق**. ص 114

[3] . غالم، محمد رضا. غانم، نذير. **التحول الرقمي للمكتبات الجامعية في ظل التكنولوجيا الناشئة بين الواقع والمأمول دراسة ميدانية: بمكتبات جامعة باتنة 1**. مجلة علوم الانسان والمجتمع. المجلد، 13. العدد، 04، 2024. ص 89

[4] . بن برغوث، ليلى. **المرجع السابق**. ص 447

[5] . غالم، محمد رضا. غانم، نذير. **المرجع نفسه**. ص 99

5.4 تحديات حوكمة المعلومات لإدارة مخاطر الأمن السيبراني في المكتبات

يعتبر التكامل بين الحوكمة والأمن السيبراني من القضايا المحورية التي تواجه المكتبات الجامعية في العصر الرقمي. فمع تزايد استخدام التقنيات الحديثة في إدارة الموارد المعلوماتية، تصبح الحاجة ملحة إلى مواءمة استراتيجيات الحوكمة مع متطلبات الأمن السيبراني لضمان الحماية الفعالة للبيانات مع الحفاظ على كفاءة وسهولة الوصول إليها. غير أن تحقيق هذا التكامل يواجه العديد من التحديات، لكنه في الوقت ذاته يتيح فرصًا كبيرة لتحسين إدارة المعلومات وتعزيز الأمن السيبراني، والمكتبات الجامعية كغيرها من المؤسسات تواجه العديد من التحديات خاصة عند محاولة الدمج بين حوكمة المعلومات والأمن السيبراني،[1] ومن أبرز هذه التحديات:

1.3.4 نقص الوعي والتدريب المتخصص في الأمن السيبراني وحوكمة المعلومات:

يُعد نقص الوعي والتدريب المتخصص أحد أكبر التحديات التي تواجه المكتبات الجامعية في تحقيق تكامل فعّال بين الحوكمة والأمن السيبراني. فمع تزايد الاعتماد على التقنيات الرقمية في إدارة البيانات والمعلومات، تبرز الحاجة إلى كوادر مؤهلة تمتلك المعرفة والمهارات اللازمة لحماية هذه الأصول الحيوية. غير أن العديد من المؤسسات الأكاديمية تعاني من فجوة في مستوى الوعي بأهمية الأمن السيبراني بين موظفي المكتبات، مما يؤدي إلى اتباع ممارسات غير آمنة قد تترك أنظمتها عرضة للهجمات الإلكترونية. على سبيل المثال، قد يقوم بعض العاملين باستخدام كلمات مرور ضعيفة، أو مشاركة بيانات حساسة دون تشفير، أو تجاهل التحديثات الأمنية لأنظمة إدارة المكتبات، وهو ما يجعلهم أهدافًا سهلة للمخترقين.[2]

من ناحية أخرى، فإن نقص التدريب المتخصص في مجال حوكمة المعلومات يؤدي إلى عدم تطبيق السياسات والمعايير الأمنية بشكل صحيح. فقد يواجه الموظفون صعوبة في فهم إجراءات الحوكمة، مثل تصنيف البيانات وفق مستويات السرية، أو الامتثال لقوانين حماية الخصوصية، أو اتباع بروتوكولات النسخ الاحتياطي والاسترداد في حالة حدوث اختراق أو فقدان البيانات. كما أن بعض المكتبات قد تعتمد على ممارسات تقليدية في إدارة المعلومات دون الاستفادة الكاملة من التقنيات الحديثة، مثل أنظمة إدارة الهوية والتحقق الثنائي[3]

---

[1] . كداوة، عبد القادر. **تحديات المكتبات الجامعية في البيئة الرقمية: خدمات المعلومات أنموذجا**. مجلة المداد. المجلد، 04. العدد، 02، 2016. ص 152

[2] . بن برغوث، ليلى. **الامن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات، واليات التصدي**. المجلة الدولية للاتصال الاجتماعي. المجلد، 10. العدد، 01، 2023. ص 451

[3] . كرمادي، شمس الدين، محمد كريم، فريحة. **واقع خدمات المعلومات بالمكتبات العامة في ظل تحديات البيئة الرقمية دراسة تحليلية: المكتبات العامة لولاية عنابة وسط**. المجلد، 26. العدد، 03، 2023. ص 400

مما يزيد من خطر تسريب البيانات أو فقدانها. التعقيد التنظيمي والتداخل بين الإدارات في المكتبات الجامعية: يُعد التعقيد التنظيمي والتداخل بين الإدارات من التحديات الأساسية التي تواجه المكتبات الجامعية عند محاولة تحقيق التكامل بين حوكمة المعلومات والأمن السيبراني. إذ تعتمد هذه المؤسسات على هياكل تنظيمية متعددة تشمل إدارات مختلفة مثل إدارة تقنية المعلومات، وإدارة المكتبات، وإدارة السياسات الأكاديمية، وكل منها قد يعمل وفق أولويات وأهداف مختلفة. وغالبًا ما يكون هناك تداخل بين مسؤوليات فرق الحوكمة، التي تُركز على وضع السياسات والمعايير الإدارية لإدارة المعلومات، وبين فرق الأمن السيبراني، التي تهدف إلى حماية هذه المعلومات من التهديدات الرقمية، مما قد يؤدي إلى تضارب السياسات أو غياب التنسيق الفعّال بينهما.[1] و على سبيل المثال، قد ترى فرق الحوكمة أن من الضروري إتاحة الوصول السهل إلى الموارد الأكاديمية للطلاب والباحثين لضمان حرية تبادل المعرفة، في حين أن فرق الأمن السيبراني قد تفرض قيودًا صارمة على الوصول إلى البيانات لمنع أي اختراق محتمل، مما يؤدي إلى صراع بين أهداف الإدارتين. بالإضافة إلى ذلك قد تعتمد بعض المكتبات الجامعية على أنظمة إدارة معلومات قديمة أو غير موحدة، حيث تستخدم أقسام مختلفة داخل نفس المؤسسة منصات مختلفة لإدارة البيانات دون وجود تكامل فعال بينها، مما يجعل من الصعب تنفيذ سياسات حوكمة موحدة أو تطبيق استراتيجيات أمنية متماسكة.[2]

علاوة على ذلك، قد يؤدي غياب إطار تنظيمي واضح يحدد المسؤوليات بين الإدارات المختلفة إلى بطء اتخاذ القرارات، وتأخير الاستجابة للتهديدات السيبرانية، وزيادة احتمالية حدوث ثغرات أمنية نتيجة سوء التنسيق. وللتغلب على هذه التحديات، تحتاج المكتبات الجامعية إلى وضع أطر تنظيمية واضحة تحدد مسؤوليات كل جهة، وتعزز التعاون بين فرق الحوكمة والأمن السيبراني من خلال منصات اتصال مشتركة، واجتماعات دورية، واعتماد سياسات موحدة توازن بين سهولة الوصول إلى المعلومات ومتطلبات الحماية السيبرانية.

2.5.4القيود المالية وضعف الاستثمار في الأمن السيبراني والتطور السريع للتهديدات السيبرانية:

تواجه المكتبات الجامعية تحديًا مزدوجًا يتمثل في محدودية الميزانيات المخصصة للأمن السيبراني والتطور السريع للتهديدات الإلكترونية، مما يجعل حماية البيانات والمعلومات الأكاديمية أكثر صعوبة. فمن ناحية، تعاني معظم المؤسسات الأكاديمية من ميزانيات محدودة تُجبرها على توجيه الإنفاق نحو الأولويات الأكاديمية مثل تطوير المناهج، وتمويل الأبحاث، وتحسين البنية التحتية التعليمية، مما يترك الأمن السيبراني في مرتبة ثانوية. نتيجة لذلك

[1] . كرمادي، شمس الدين، محمد كريم، فريحة. **واقع خدمات المعلومات بالمكتبات العامة في ظل تحديات البيئة الرقمية دراسة تحليلية: المكتبات العامة لولاية عنابة وسط**. المجلد، 26. العدد، 03، 2023. ص 400

[2] . كرمادي، شمس الدين. محمد كريم، فريحة. **المرجع نفسه**. ص 442-443

لا يتم تخصيص موارد كافية لتحديث أنظمة الحماية، أو اقتناء برمجيات متقدمة للكشف عن الهجمات السيبرانية[1]، أو الاستثمار في تقنيات مثل التشفير المتقدم، أو تأمين منصات الحوسبة السحابية التي أصبحت جزءًا أساسيًا من بيئة المكتبات الحديثة. بالإضافة إلى ذلك، فإن ضعف الميزانية يؤثر على قدرة المؤسسات على تقديم برامج تدريبية متخصصة لموظفي المكتبات، مما يؤدي إلى نقص الكفاءات القادرة على التعامل مع المخاطر السيبرانية بكفاءة.[2]

من ناحية أخرى، تتطور التهديدات السيبرانية بوتيرة متسارعة، حيث أصبحت الهجمات الإلكترونية أكثر تعقيدًا وتنوعًا، بدءًا من هجمات التصيد الاحتيالي (Phishing) التي تستهدف موظفي المكتبات والباحثين، مرورًا بهجمات الفدية (Ransomware) التي يمكن أن تشل أنظمة المكتبة بالكامل، وصولًا إلى الاختراقات المتقدمة التي تستهدف سرقة البيانات الحساسة أو تعطيل الخدمات الأكاديمية. وفي كثير من الحالات، لا تتمكن المكتبات الجامعية من مواكبة هذه التهديدات بسبب نقص الموارد المالية والتقنية، مما يجعلها عرضة للاختراقات الأمنية التي قد تؤدي إلى فقدان بيانات قيمة أو انتهاك خصوصية المستخدمين. علاوة على ذلك، فإن تحديث أنظمة الأمن السيبراني بشكل دوري يتطلب استثمارات مستمرة في الأجهزة والبرمجيات والخبرات البشرية، وهو أمر قد يكون صعب التحقيق في ظل القيود المالية الصارمة.[3]

3.5.4التوازن بين الأمن السيبراني وسهولة الوصول إلى المعلومات في المكتبات الجامعية:

يعد تحقيق التوازن بين متطلبات الأمن السيبراني وسهولة الوصول إلى المعلومات من أكبر التحديات التي تواجه المكتبات الجامعية، نظرًا لطبيعة دورها في توفير المعرفة بأكبر قدر من الانفتاح والشفافية. فمن جه ة، تتطلب معايير الأمن السيبراني فرض قيود صارمة لحماية البيانات من الاختراقات والتهديدات الإلكترونية، مثل تقييد صلاحيات الوصول إلى المعلومات، وتطبيق تقنيات التشفير، واستخدام إجراءات تحقق متعددة الطبقات، مما قد يُعيق سرعة وصول الطلاب والباحثين إلى المصادر الأكاديمية التي يحتاجونها. ومن جهة أخرى، تهدف المكتبات الجامعية إلى تسهيل الوصول الحر إلى المعلومات، وتمكين الباحثين من استكشاف المحتوى بسهولة، مما قد يتعارض مع بعض الإجراءات الأمنية التي تفرض قيودًا إضافية على المستخدمين.[4]

---

[1] . كرمادي، شمس الدين. محمد كريم، فريحة. **المرجع نفسه**. ص 442-443

[2] . زواوي، لمياء. رملي، فهيم. **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**. المجلة الجزائرية للأمن والتنمية. المجلد، 12. العدد، 02، 2023. ص 151-152

[3] . العيداني، محمد. **التهديدات السيبرانية وجرائم المعلومات**. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المجلد، 13. العدد، 01، 2024. ص 17-18

[4] . بوقنادل، عبد اللطيف. ماحي، أمين. **المكتبة الرقمية ودورها في تطوير البحث العلمي**. المجلة الجزائرية للعلوم القانونية والسياسية. المجلد، 57. العدد، 03، 2020. ص 176-178

على سبيل المثال، قد تتطلب بعض أنظمة الحماية تسجيل الدخول باستخدام إجراءات تحقق متعددة العوامل (MFA)، أو فرض قيود على تحميل أو مشاركة بعض المستندات، أو حتى تقييد الوصول إلى موارد معينة بناءً على تصنيفات المستخدمين (مثل الطلاب، الباحثين، أو أعضاء هيئة التدريس). ورغم أهمية هذه الإجراءات لحماية البيانات من الاستخدام غير المشروع أو الاختراقات، إلا أنها قد تُشَكِّل عائقًا أمام الباحثين الذين يحتاجون إلى وصول سريع وغير مقيد إلى المصادر العلمية. بالإضافة إلى ذلك، قد تؤدي بعض السياسات الأمنية المشددة إلى تقليل تجربة المستخدم، مما يدفع البعض إلى البحث عن طرق بديلة وغير آمنة للوصول إلى المعلومات، مثل مشاركة بيانات تسجيل الدخول أو استخدام شبكات غير محمية.[1] رغم التحديات السابقة، هناك العديد من الفرص التي يمكن أن تساهم في تعزيز التكامل بين الحوكمة والأمن السيبيراني وتتمثل هده الفرص فيما يلي:

❖ تبني سياسات حوكمة مرنة ومتطورة:

تحتاج المكتبات الجامعية إلى تبني نهج مرن يحقق التوازن بين الحماية الفعالة وسهولة الاستخدام. يمكن ذلك من خلال تطبيق سياسات أمنية ذكية تعتمد على تصنيف مستويات الحساسية للمعلومات، بحيث يتم فرض قيود أكثر صرامة على البيانات الحساسة، مع السماح بالوصول السلس إلى المحتوى العام. كما يمكن استخدام تقنيات مثل التحقق الذكي من الهوية، الذي يُمَكِّن المستخدمين من الوصول إلى المعلومات بناءً على موقعهم أو جهازهم، بحيث لا يتم تطبيق نفس مستوى الأمان الصارم على جميع الحالات. بالإضافة إلى ذلك، فإن رفع مستوى الوعي بين الطلاب والباحثين حول أهمية الأمن السيبراني وأفضل الممارسات في حماية البيانات يمكن أن يساهم في تحقيق بيئة متوازنة تجمع بين الانفتاح الأكاديمي والحماية الفعالة للموارد الرقمية.[2]

❖ استخدام التقنيات الحديثة في تأمين المعلومات وتعزيز التكامل بين الحوكمة والأمن السيبيراني:

يُعتبر تبني التقنيات الحديثة، مثل الذكاء الاصطناعي والتعلم الآلي، فرصة كبيرة لتعزيز الأمن السيبراني في المكتبات الجامعية وتحقيق تكامل أفضل مع مبادئ حوكمة المعلومات. فمع تزايد حجم البيانات الرقمية التي تديرها المكتبات، أصبح من الضروري الاستعانة بتقنيات قادرة على تحليل الأنماط السلوكية للمستخدمين، واكتشاف التهديدات المحتملة قبل أن تتسبب في أضرار فعلية. ويمكن توضيح ذلك في النقاط الاتية:[3]

---

[1] . بوقنادل، عبد اللطيف. ماحي، أمين. **المرجع السابق**. ص 200

[2] . بوقنادل، عبد اللطيف. ماحي، أمين. **المرجع نفسه**. ص 223

[3] . كداوة، عبد القادر. **تأثير تكنولوجيا المعلومات على خدمات المكتبات الجامعية المركزية الجزائرية: جامعات الجزائر الوسط أنموذجا**. مجلة الدراسات والأبحاث، المجلد، 08. العدد، 24، 2016. ص 164-165

- يُستخدم في تطوير أنظمة مراقبة متقدمة قادرة على رصد النشاطات غير الطبيعية، مثل محاولات تسجيل الدخول غير المصرح بها، أو تحميل كميات كبيرة من البيانات بشكل مفاجئ، أو محاولات الوصول إلى معلومات محمية من قبل جهات غير مخولة.
- يمكن لأنظمة التعلم الآلي تحسين قدرة المكتبات على التمييز بين السلوكيات الطبيعية للمستخدمين وتلك التي قد تشير إلى تهديدات أمنية، مما يتيح استجابة أسرع وأكثر دقة للهجمات الإلكترونية.
- تتيح هذه التقنيات إمكانية تحسين أنظمة إدارة الهوية والوصول (IAM)، بحيث يتم التحكم في صلاحيات المستخدمين بناءً على عوامل متعددة مثل الموقع الجغرافي، أو نوع الجهاز المستخدم، أو السجل السلوكي السابق، مما يعزز أمن المعلومات دون التأثير سلبًا على تجربة المستخدم.
- تعزيز إجراءات التشفير والحماية التلقائية للبيانات، حيث تقوم الأنظمة بتحليل المخاطر وتطبيق سياسات أمان مخصصة وفقًا لمستوى حساسية المعلومات. ومن الناحية الإدارية، تساهم هذه التقنيات في دعم حوكمة المعلومات من خلال أتمتة عمليات الامتثال للمعايير والسياسات التنظيمية، مما يقلل من الأخطاء البشرية ويعزز كفاءة إدارة البيانات. [1]

وبهذا، فإن اعتماد التقنيات الحديثة في المكتبات الجامعية لا يقتصر فقط على تعزيز الأمن السيبراني، بل يُسهم أيضًا في تحقيق إدارة أكثر ذكاءً وكفاءةً للمعلومات، لهذا يعد الذكاء الاصطناعي ضروريًا لتحديد التهديدات غير المعروفة في مجال الأمن السيبراني، حيث يمكنه تحليل كميات هائلة من البيانات بكفاءة لاكتشاف الحالات الشاذة. كثيراً ما يغير المتسللون تكتيكاتهم، مما يجعل من الصعب على الأنظمة التقليدية مواكبة ذلك. يستفيد الذكاء الاصطناعي من التعلم الآلي للتعرف على الأنماط واكتشاف السلوك غير المعتاد، حتى لو لم يسبق له مثيل من قبل. تعتبر هذه القدرة ضرورية لتحديد التهديدات بشكل استباقي والتي يمكن أن تسبب أضرارًا كبيرة إذا تركت دون أن يلاحظها أحد، مما يوفر دفاعًا قويًا ضد التهديدات السيبرانية المتطورة.[2] ومن بين الأدوار التي يلعبها الذكاء الاصطناعي في تعزيز الأمن السيبيراني:

[1] . بن برغوث، ليلى. **المرجع السابق**. ص 455

[2] . كداوة، عبد القادر. **المرجع نفسه**. ص 168

- التعامل مع كميات هائلة من البيانات: من المزايا المهمة للذكاء الاصطناعي في مجال الأمن السيبراني قدرته على التعامل مع كميات كبيرة من البيانات. تولد الشبكات الحديثة قدرًا هائلاً من حركة المرور، ويعتبر تحليل هذه البيانات يدويًا أمرًا غير عملي بالنسبة للخبراء البشريين. يمكن للذكاء الاصطناعي التدقيق في هذه البيانات بكفاءة، وتحديد التهديدات المحتملة المخفية داخل حركة المرور العادية. لا تعمل هذه الأتمتة على تعزيز اكتشاف التهديدات فحسب، بل تضمن أيضًا تحديد التهديدات والتخفيف من حدتها بسرعة، مما يحافظ على أمن الشبكة وسلامتها.[1]

- التعلم المستمر والتكيف: تتحسن أنظمة الذكاء الاصطناعي بمرور الوقت من خلال التعلم المستمر والتكيف. باستخدام تقنيات مثل التعلم الآلي والتعلم العميق، يمكن للذكاء الاصطناعي دراسة سلوك الشبكة وتحديد الانحرافات عن القاعدة. تتيح هذه القدرة للذكاء الاصطناعي الاستجابة فورًا للتهديدات وتحسين خوارزميات الكشف الخاصة به للحوادث المستقبلية. ومن خلال التعلم المستمر من كل تفاعل، يجعل الذكاء الاصطناعي من الصعب على نحو متزايد على المتسللين ابتكار استراتيجيات يمكنها تجاوز التدابير الأمنية، وضمان حماية قوية. علاوة على ذلك، تسمح عملية التعلم التكيفية للذكاء الاصطناعي بالبقاء في صدارة التهديدات الناشئة من خلال تطوير منهجيات الكشف الخاصة به، مما يجعله عنصرًا حاسمًا في استراتيجيات الأمن السيبراني الحديثة.[2]

- تعزيز إدارة الثغرات الأمنية: يلعب الذكاء الاصطناعي دورًا حاسمًا في إدارة الثغرات الأمنية من خلال التحليل المستمر لإجراءات أمان الشبكة لتحديد نقاط الضعف. يسمح هذا النهج الاستباقي للمؤسسات بمعالجة نقاط الضعف قبل أن يتم استغلالها من قبل مجرمي الإنترنت. إن قدرة الذكاء الاصطناعي على تحديد أولويات نقاط الضعف بناءً على التأثير المحتمل تساعد فرق الأمان على التركيز على التهديدات الأكثر أهمية، وتحسين أمان الشبكة بشكل عام وتقليل مخاطر الانتهاكات. علاوة على ذلك، يمكن للذكاء الاصطناعي أتمتة عمليات فحص الثغرات الأمنية وإدارة التصحيحات، مما يضمن معالجة جميع نقاط الضعف المعروفة على الفور، مما يعزز بشكل كبير مرونة البنية التحتية لتكنولوجيا المعلومات ضد التهديدات السيبرانية المحتملة.[3]

---

[1] . مريم، فاطمة الزهراء. **الذكاء الاصطناعي والمكتبات: مراجعة الأدبيات**. مجلة علم المكتبات والمعلومات. المجلد، 16. العدد، 01، 2024. ص 563

[2] . مريم، فاطمة الزهراء. **المرجع السابق**. ص 565

[3] . سعيدي، خليل. بن مهدي، مرزوق. **الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبيراني: واقع اليوم ورهان الغد**. مجلة السلام للعلوم الإنسانية والاجتماعية. المجلد، 06. العدد، 01، 2022. ص 26 – 28

- تقليل العمليات المتكررة: يقلل الذكاء الاصطناعي بشكل كبير من عبء المهام الأمنية المتكررة على موظفي الأمن السيبراني. ومن خلال أتمتة المهام الروتينية، مثل البحث عن التهديدات الأمنية الأساسية وإجراء تحليلات تفصيلية، يسمح الذكاء الاصطناعي للخبراء البشريين بالتركيز على القضايا الأمنية الأكثر تعقيدًا. لا تعمل هذه الأتمتة على تحسين الكفاءة فحسب، بل تضمن أيضًا اتباع أفضل الممارسات في مجال أمن الشبكات باستمرار، مما يقلل من مخاطر الأخطاء البشرية.[1]

- تسريع أوقات الكشف والاستجابة: يؤدي دمج الذكاء الاصطناعي في ممارسات الأمن السيبراني إلى تسريع اكتشاف التهديدات والاستجابة لها. يمكن لأنظمة الذكاء الاصطناعي فحص الشبكات بأكملها، وتحديد التهديدات مبكرًا، وأتمتة إجراءات الاستجابة، مما يقلل الوقت المستغرق لتخفيف الأضرار المحتملة. وتعد هذه الاستجابة السريعة أمرًا بالغ الأهمية في منع الأضرار التي لا يمكن إصلاحها الناجمة عن الهجمات السيبرانية، وضمان تنفيذ التدابير الأمنية بسرعة وفعالية. من خلال أتمتة الكشف عن التهديدات والاستجابة لها، يعزز الذكاء الاصطناعي مرونة فرق الأمن، مما يسمح لهم بالتركيز على المهام الإستراتيجية وتحسين المرونة العامة لموقف الأمن السيبراني للمؤسسة.[2]

- تأمين عمليات المصادقة: يعمل الذكاء الاصطناعي على تحسين عمليات المصادقة عن طريق إضافة طبقة إضافية من الأمان من خلال أدوات مثل التعرف على الوجه، واختبار CAPTCHA، وماسحات بصمات الأصابع. تساعد هذه التقنيات في التحقق من هويات المستخدم أثناء محاولات تسجيل الدخول، مما يمنع الوصول غير المصرح به. من خلال الكشف عن محاولات تسجيل الدخول الاحتيالية ومنع حشو بيانات الاعتماد وهجمات القوة الغاشمة، يضمن الذكاء الاصطناعي أن المستخدمين الشرعيين فقط هم من يمكنهم الوصول إلى المعلومات الحاسة. علاوة على ذلك، تتعلم أنظمة المصادقة المعتمدة على الذكاء الاصطناعي باستمرار التهديدات الجديدة وتتكيف معها، مما يعزز قدرتها على اكتشاف ومنع الهجمات السيبرانية المعقدة التي تهدف إلى المساس ببيانات اعتماد المستخدم.[3]

---

[1] . الجزيرة " الجزيرة نت". **تقنيات الأمن السيبراني والتحديات المستقبلية**. تاريخ الولوج: 16-03-2025 على 20:30 متاح على الرابط www.aljazeera.net

[2] . سعيدي، خليل. بن مهدي، مرزوق. **المرجع نفسه**. ص 35

[3] . الجزيرة " الجزيرة نت". **قراءة في كتاب "الامن السيبراني المخاطر والتحديات والمواجهة**. تاريخ الولوج: 16-03-2025 على 20:50 متاح على الرابط www.aljazeera.net

- كشف التهديدات والوقاية منها: يتفوق الذكاء الاصطناعي في اكتشاف التهديدات والوقاية منها من خلال تحليل مجموعات البيانات الكبيرة وتحديد الأنماط غير العادية التي قد تشير إلى هجمات إلكترونية. عند اكتشاف تهديد محتمل، تطلق أنظمة الذكاء الاصطناعي تنبيهات في الوقت الفعلي لفرق الأمان، مما يتيح استجابات سريعة. ويقلل هذا النهج الاستباقي من فرص استغلال المهاجمين لنقاط الضعف، مما يضمن تخفيف التهديدات قبل أن تتسبب في ضرر كبير.[1]

- كشف البرامج الضارة والتصيد: تعمل الأنظمة المستندة إلى الذكاء الاصطناعي على تحسين اكتشاف البرامج الضارة والتصيد الاحتيالي بشكل كبير من خلال تحليل محتوى البريد الإلكتروني وسياقه للتمييز بين الرسائل المشروعة والتهديدات. تعمل خوارزميات التعلم الآلي على تمكين الذكاء الاصطناعي من التكيف مع التهديدات الجديدة، والتعرف على الهجمات المعقدة مثل التصيد الاحتيالي. من خلال اعتراض الأنشطة المشبوهة في وقت مبكر، يمنع الذكاء الاصطناعي الضرر المحتمل لشبكات الشركات ويعزز الأمن العام.[2]

- تحليل سجل الأمان: يقوم الذكاء الاصطناعي بتحويل تحليل سجل الأمان من خلال استخدام خوارزميات التعلم الآلي لاكتشاف الأنماط والشذوذات في بيانات السجل في الوقت الفعلي. تتيح هذه القدرة للمؤسسات التعرف بسرعة على الخروقات الأمنية المحتملة والاستجابة لها، حتى بدون وجود تهديدات معروفة. بالإضافة إلى ذلك، يتفوق الذكاء الاصطناعي في اكتشاف التهديدات الداخلية من خلال التحليل الشامل لسلوك المستخدم، مما يضمن حماية قوية ضد التهديدات الداخلية والخارجية. من خلال أتمتة تحليل سجلات الأمان، يساعد الذكاء الاصطناعي فرق الأمان على تحديد الأنشطة المشبوهة ومعالجتها بسرعة، مما يعزز الكفاءة العامة لجهود الكشف عن التهديدات والاستجابة لها.[3]

---

[1] . مريم، فاطمة الزهراء. **المرجع السابق**. ص 564

[2] . الجزيرة " الجزيرة نت". **تقنيات الأمن السيبراني والتحديات المستقبلية**. تاريخ الولوج: 16-03-2025 على: 21:11 متاح على الرابط: www.aljazeera.net

[3] . لجزيرة " الجزيرة نت". **المرجع نفسه**.

- استخبارات التهديدات السيبرانية بمساعدة الذكاء الاصطناعي: تستفيد استخبارات التهديدات السيبرانية (CTI) من قدرة الذكاء الاصطناعي على التعامل مع المهام الروتينية، وتنظيم البيانات، وتقديم رؤى قابلة للتنفيذ. يمكن للذكاء الاصطناعي/التعلم الآلي تعزيز CTI من خلال جمع المعلومات حول الهجمات والأحداث السيبرانية، مما يساعد فرق الأمان على الاستعداد للتهديدات المحتملة قبل حدوثها. من خلال أتمتة جمع البيانات وتحليلها، يتيح الذكاء الاصطناعي لمحترفي الأمن التركيز على اتخاذ القرارات الإستراتيجية والاستجابة بفعالية للتهديدات الحالية. [1]

- مسح الكود بمساعدة الذكاء الاصطناعي: يعمل الذكاء الاصطناعي على تحسين اختبار أمان التطبيقات الثابتة (SAST) واختبار أمان التطبيقات الديناميكي (DAST) بشكل كبير من خلال تقليل النتائج الإيجابية الخاطئة وتوفير تحليل مدرك للسياق. يساعد الذكاء الاصطناعي في مراجعة التعليمات البرمجية وفحص الثغرات الأمنية، مما يساعد المطورين على اكتشاف الأخطاء قبل الإرسال. تعمل هذه الأتمتة على تحرير الموارد البشرية لمشاريع وابتكارات أكثر قيمة، مما يعزز أمان البرامج بشكل عام. بالإضافة إلى ذلك، فإن قدرة الذكاء الاصطناعي على التعلم المستمر والتكيف مع ممارسات الترميز الجديدة تضمن بقاءه فعالاً في تحديد نقاط الضعف والتخفيف منها، مما يوفر حماية قوية ضد الخروقات الأمنية المحتمل.[2]

وبالتالي يمكن القول ان أحد أبرز التحديات التي تواجه الأمن السيبراني اليوم هو اتساع الفجوة بين المؤسسات الكبيرة والصغيرة في القدرة على الصمود أمام الهجمات السيبرانية. فبينما تمتلك الشركات الكبرى موارد مالية وتقنية متقدمة تتيح لها تعزيز دفاعاتها السيبرانية، تفتقر المؤسسات الصغيرة والمتوسطة إلى الإمكانات اللازمة لمواكبة هذا التصاعد في التهديدات، ما يجعلها نقاط ضعف تُستغل لضرب سلاسل التوريد بأكملها وهذا ما تشير اليه الإحصاءات إلى أن 35% من المؤسسات الصغيرة ترى أن قدرتها على التصدي للهجمات السيبرانية غير كافية، وهو ما يعكس اتساع هذه الفجوة مقارنة بالسنوات السابقة.[3]

---

[1] . مريم، فاطمة الزهراء. **المرجع السابق**. ص 566

[2] . سهلي، مراد. **توظيف تقنيات الذكاء الاصطناعي في تحسين أداء المكتبات الجامعية: دراسة ميدانية بالمكتبات الجامعية بجامعة محمد خيضر بسكرة**. مجلة دراسات وأبحاث. المجلد، 17. العدد، 01، 2025. ص 156 -158

[3]. ELzidi, Sulaiman. **Harnessing the power pf Artificial Intelligence Applications in Academic Library Information Services**. The Bibliography Journal for Library and Information studies. Vol,06. Nu,01, 2024. P 79

وفقًا لتقديرات شركة Market and Market المتخصصة في بحوث السوق، فقد بلغ حجم صناعة الأمن السيبراني عالميًا نحو 190.5 مليار دولار في عام 2023. وتشير بيانات The Business Research Company، الى أنّ الإنفاق على الأمن السيبراني ارتفع إلى 243.15 مليار دولار في عام 2024، ومن المتوقع أن يصل إلى 267 مليار دولار بنهاية عام 2025. يعكس هذا النمو المتسارع تصاعد التهديدات السيبرانية وزيادة الوعي بأهمية الأمن السيبراني، مما يدفع الحكومات والشركات إلى تكثيف استثماراتها في هذا المجال لحماية بنيتها التحتية الرقمية وضمان استمرارية أعمالها في بيئة رقمية متزايدة التعقيد.[1]

❖ تعزيز التعاون بين المؤسسات الأكاديمية والشركات التقنية في مجال الأمن السيبراني:

يُعَدّ التعاون بين المكتبات الجامعية والمؤسسات الأكاديمية الأخرى، بالإضافة إلى الشراكة مع الشركات المتخصصة في الأمن السيبراني، أحد أهم الفرص لتعزيز الحماية الرقمية وتحقيق تكامل فعّال بين حوكمة المعلومات والأمن السيبراني. ففي ظل تزايد التهديدات الإلكترونية وتعقيد أساليب الهجمات السيبرانية، لم يعد من الممكن الاعتماد فقط على الجهود الفردية لكل مؤسسة، بل أصبح من الضروري تبادل الخبرات والمعرفة بين الجهات المختلفة لمواكبة أحدث التطورات في مجال الحماية الرقمية ويمكن أن يتم ذلك من خلال:

- إنشاء تحالفات مع جامعات أخرى لمشاركة الموارد الأمنية، مثل: قواعد البيانات الخاصة بالتهديدات السيبرانية، وأدوات تحليل المخاطر، واستراتيجيات الاستجابة للهجمات.
- تنظيم ورش عمل مشتركة، ومؤتمرات علمية متخصصة، وبرامج تدريبية تستهدف موظفي المكتبات ومسؤولي تقنية المعلومات، مما يساهم في رفع مستوى الوعي وتعزيز القدرات الأمنية داخل المؤسسات الأكاديمية.
- الاستفادة من الأبحاث الأكاديمية في مجال الأمن السيبراني لتطوير حلول جديدة تتناسب مع احتياجات المكتبات، مثل أنظمة التحقق المتقدمة، وتقنيات التشفير، وأدوات الكشف عن التهديدات في الوقت الفعلي.
- التعاون مع الشركات التقنية المتخصصة، يمكن أن يوفر للمكتبات إمكانية الوصول إلى أحدث الحلول الأمنية، مثل برامج الحماية من الفيروسات، وأنظمة إدارة الهوية، وخدمات الأمن السحابية[2].

---

[1] . الجزيرة " الجزيرة نت". **قراءة في كتاب "الامن السيبراني المخاطر والتحديات والمواجهة**. تاريخ الولوج: 16-03-2025 على 22:30 متاح على الرابط www.aljazeera.net

[2] . محمد كريم، فريحة. كرمادي، شمس الدين. **واقع خدمات المعلومات بالمكتبات العامة في ظل تحديات البيئة الرقمية دراسة تحليلية: المكتبات العامة لولاية عتابة وسط**. مجلة التواصل. المجلد، 26. العدد، 03، 2023. ص 400

- كما أن هذه الشركات غالبًا ما تمتلك فرقًا متخصصة في تحليل التهديدات وتقديم استشارات أمنية، مما يسمح للمكتبات الجامعية بتحسين استراتيجياتها الأمنية وتطوير خطط استجابة فعالة للحوادث مما تساهم في أن تساعد المكتبات على التغلب على القيود المالية، من خلال الاستفادة من العروض المخفضة أو البرامج الأكاديمية التي تقدمها الشركات الكبرى لدعم المؤسسات التعليمية.[1]

وبهذا، فإن تعزيز التعاون بين المكتبات الجامعية، المؤسسات الأكاديمية الأخرى، والشركات التقنية لا يُسهم فقط في تحسين مستوى الأمن السيبراني، بل يساعد أيضًا في تحقيق إدارة أكثر كفاءة للمعلومات، وتوفير بيئة بحثية آمنة تدعم الابتكار والمعرفة.

❖ دمج التدريب والتوعية في سياسات المكتبات لتعزيز الأمن السيبراني وحوكمة المعلومات:

يُعَدّ دمج التدريب والتوعية في سياسات المكتبات الجامعية أحد العوامل الأساسية لتحقيق التكامل الفعّال بين الحوكمة والأمن السيبراني. ف مع تزايد التهديدات الإلكترونية وتعقيدها، يصبح الوعي الأمني لدى العاملين والطلاب عنصرًا حاسمًا في حماية البيانات الشخصية والمؤسسية. وغالبًا ما تكون الهجمات السيبرانية ناجحة بسبب الأخطاء البشرية، مثل استخدام كلمات مرور ضعيفة، أو مشاركة بيانات حساسة عن غير قصد، أو الوقوع في فخ عمليات التصيد الاحتيالي (Phishing) ولذلك، فإن تضمين برامج تدريبية مستمرة في سياسات المكتبات يمكن أن يُحدث تحولًا كبيرًا في طريقة تعامل المستخدمين مع البيانات والأنظمة الرقمية. لهذا يمكن للمكتبات الجامعية تطوير استراتيجيات تدريبية متعددة المستويات تستهدف فئات مختلفة من المستخدمين.[2] فعلى سبيل المثال:

- توفير دورات تدريبية مكثفة لموظفي المكتبات حول كيفية تطبيق سياسات الحوكمة، وإدارة الوصول إلى المعلومات، والتعامل مع حوادث الاختراق السيبراني.
- تقديم ورش عمل دورية للطلاب وأعضاء هيئة التدريس لتعريفهم بأفضل الممارسات في تأمين حساباتهم، وحماية أجهزتهم من البرمجيات الضارة، والتعامل بحذر مع رسائل البريد الإلكتروني المشبوهة والروابط غير الموثوقة.[3]

---

[1] . محمد كريم، فريحة. كرمادي، شمس الدين. **المرجع السابق**. ص 402

[2] . رايس، عبد الوهاب. صغيري، ميلود. **المرجع السابق**. ص 100-101

[3] . الحسيني، فايزة. **الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية**. مجلة البحث العلمي. المجلد، 13. العدد، 02، 2023. ص 56 -57

- دمج التوعية بالأمن السيبراني ضمن عمليات تسجيل الدخول إلى الأنظمة الأكاديمية، من خلال تقديم نصائح أمنية قصيرة أو اختبارات تفاعلية لرفع مستوى الوعي بشكل مستمر.
- الاستفادة من تقنيات الذكاء الاصطناعي في تخصيص برامج التدريب بناءً على سلوك المستخدمين، بحيث يتم تقديم محتوى توعوي مناسب لكل فرد بناءً على تاريخه في استخدام الأنظمة الرقمية. كما يمكن تعزيز التوعية من خلال حملات توعوية على منصات التواصل الاجتماعي ولوحات الإعلانات داخل الحرم الجامعي، مما يضمن وصول المعلومات الأمنية إلى أكبر عدد ممكن من المستفيدين.

وبهذا، فإن دمج التدريب والتوعية في سياسات المكتبات لا يسهم فقط في تقليل المخاطر السيبرانية، بل يعزز أيضًا ثقافة الأمن الرقمي والمسؤولية المشتركة، مما يجعل المكتبات الجامعية بيئة أكثر أمانًا وانضباطًا في إدارة المعلومات وحمايتها.

يشهد مستقبل حوكمة المعلومات والأمن السيبيراني في المكتبات الجامعية تطورا متسارعا لمواكبة التحديات الرقمية المتزايدة. مع تزايد حجم البيانات الرقمية أصبحت المكتبات الجامعية بحاجة الى استراتيجيات متقدمة لإدارة المعلومات وضمان حمايتها من التهديدات السيبرانية كالقرصنة الالكترونية، وتسريب البيانات، وأيضا الهجمات الخبيثة، والتي تعتمد على سياسة تنظيمية واضحة من أجل إدارة المعلومات والبيانات البحثية مثل: التحكم في الوصول الى البيانات، وتطبيق تقنيات التشفير، وتعزيز الوعي الأمني بين المستخدمين. في المقابل يسهم الامن السيبيراني في حماية الأنظمة من الهجمات الالكترونية عن طريق عدة أشكال مثل استخدام تقنيات الذكاء الاصطناعي والتحليل التنبئي، لهذا من المتوقع ان تتبنى المكتبات الجامعية نهجا استباقيا يستند الى الابتكار التكنولوجي والتعاون مع الهيئات الاكاديمية لتطوير حلول أمنية متكاملة، كما ستوفر الحوسبة السحابية بيئة أكثر أمانا لإدارة الموارد الالكترونية إضافة الى ذلك ستعتمد المكتبات على التحليلات الضخمة لتوقع التهديدات واتخاذ التدابير الوقائية بشكل استباقي. وبالتالي يمكن القول ان مستقبل حوكمة المعلومات والامن السيبيراني في المكتبات الجامعية يتطلب استراتيجيات متكاملة تستند إلى التكنولوجيا الحديثة والسياسات الصارمة، مما يضمن حماية المعرفة الأكاديمية واستدامة الخدمات الرقمية في بيئة امنة وموثوقة[1].

[1] . الحسيني، فايزة. **المرجع نفسه**. ص60

الفصل الرابع: دور حوكمة المعلومات في التقليل من مخاطر الأمن السيبراني في المكتبات الجامعية

خلاصة الفصل:

أصبحت المكتبات الجامعية في ظل التحول الرقمي، تعتمد بشكل متزايد على النظم الإلكترونية في إدارة مواردها وخدماتها، مما جعل المعلومات أحد أهم أصولها الإستراتيجية. ومنه حوكمة المعلومات كإطار تنظيمي يحدد

السياسات والإجراءات والأدوار والمسؤوليات المتعلقة بإدارة المعلومات بما يضمن حمايتها وسلامتها وأمنها.

وترتبط حوكمة المعلومات ارتباطًا وثيقًا بالأمن السيبراني، ذلك أن تطبيق مبادئ الحوكمة يلعب دور هام في تقليل مخاطر التهديدات السيبرانية. كما تساعد الحوكمة على تحقيق التوازن بين إتاحة المعلومات للمستفيدين وحمايتها من الاختراق أو التسريب أو التلاعب.الأمر الذي يجعل الأمن السيبيراني يعد أحد الركائز التنفيذية لحوكمة المعلومات في المكتبات الجامعية.

الفصل الخامس

الدراسة الإستطلاعية:

المؤشرات والنتائج

تمهيد:

خصص الجانب الميداني للدراسة؛ الفصل الأول الإشارة إلى المكتبات الجامعية والدور المحوري الذي تلعبه في مؤسسات التعليم العالي والبحث العلمي مع الإشارة إل أبرز خدمات المعلومات المقدمة لمجتمع المستفيدين.فيما جاء الإطار العام للفصل في تحديد وتوضيح مخطط الدراسة الإستطلاعية كونها موجعية الباحث في الدراسة الأساسية، وتحديد إجراءات الدراسةالإستطلاعية ومخرجاتها.

1.5 تعريف المكتبات الجامعية الجزائرية

تعد المكتبات الجامعية من أهم أنواع المكتبات لما لها من إرتباط وثيق بالمؤسسات العلمية والبحثية التي تتبع منهج أكاديمي وبرامج تكوين متنوعة في مختلف التخصصات العلمية،ولطالما كانت المصدر الأول للمعلومات عند الطلبة والباحثيين.

وإذا تتبعا البعد التاريخي للمكتبات الجامعية نجد بأنها: "مكان يحتوي مجموعة من الكتب والمواد المحفوظة للقراءة أو الدراسة أو الإستشارة:"[1]، وهذا الفكر يرتبط إرتباطا وثيقا بالبيئة التي تحيط بالمقتنيات في القديم وأيضا غياب المؤسسات البحثية وخصوصا أن المكتبة إرتبط وجودها بالمؤسسات المهتمة بالتعليم والنشر.

ومع التحولات والتطورات التكنولوجية نتيجة الإنفجار المعلوماتي وما تبعه من إبتكارات تكنولوجية ومع تزايد قيمة المعلومات وظهور الجامعة كمؤسسة ومنظومة لها كيان مستقل تغيرت نظرة المكتبات الجامعية من الناحية المفاهيمية والوظيفية، عرفت المكتبة الجامعية بأنها: "المكان أين تقدم فيه أحسن خدمة مكتبية ومعلوماتية كونها تتفاعل مع النخبة في المجتمع، تقع عليها مسؤولية توفير كل أنواع المعلومات لتلبية حاجات القراء"[2].

ويعرفها الهمشري بأنها:" نوع متميز من المكتبات الأكاديمية وهي المكتبو أو مجموعة المكتبات التي تقوم الجامعات بإنشائها وتمويلها وإدارتها من أجل تقديم الخدمات المعلوماتية للمستفيدين في المجتمع بما يتفق وأهداف الجامعة"[3]

وفي ضوء ما سبق يمكن تعريف المكتبات الجامعية بأنها: مؤسسة علمية بحثية تابعة لوزارة التعليم العالي والبحث العلمي، تعد أحد المرافق المعرفية الهامة في الجامعة. تخضع المكتبات الجامعية للإدارة المركزية. تسهم في

---

[1]. برابح إسمهان. **جاهزية المكتبات الجامعية ودورها في تطبيق اليقضة المعلوماتية لدى أخصائي المعلومات: دراسة ميدانية بمؤسسات التعليم العالي والبحث العلمي ولاية عنابة**، أطروحة دكتوراه، تخصص علم المكتبات، جامعة عنابة، 2020.ص.37

[2]. فردي، لخضر. **المكتبات الجامعية في ظل مجتمع المعلومات: نحو التكيف مع التحديات**. مجلة العلوم الإنسانية: مجلد أ، العدد 28، 2007.ص.104.

[3]. الهمشري، عمر أحمد؛ عليان، ربحي مصطفى. **المرجع في علم المكتبات والمعلومات**. عمان:دار الشروق، 1996.ص45

دعم البحث العلمي وتوفير موارد معرفية تتلائم مع برامج التكوين في مختلف التخصصات العلمية بهدف تلبية الأسرة الجامعية.

1.1.5 المكتبات الجامعية والتكنولوجيا الجديدة

عرف العالم تطورات وتحولات تكنولوجية ومعرفية وتقنية أفرزت ظهور تكنولوجيا جديدة، خلقت بصمة في عالم التقنية لما تتميز به من حداثة وفعالية. بدأت بظهور الحواسيب ونظم المعلومات إلى الشبكة العنكبوتية العالمية، هذه الأخيرة أصبحت المصدر الأول للمعلومات لما تملكه خصائص وإمكانيات وما توفره من رفع للفواصل والحدود المكانية والزمانية.

هذا التغيير كان له أثر كبير على جميع مناحي الحياة، وشمل أيضا المكتبات الجامعية التي أصبحت تشكل قاعدة بيانات وشبكة معلومات تلبي إحتياجات المستفيدين في مختلف التخصصات العلمية، فإنتقل بذلك دورها من

تنظيم المقتنيات إلى إتاحة مصادر المعلومات، ومن إستخدام الرف إلى الحضور الرقمي في صفحات الويب والإتصال المباشر مع المستفيدين[1].

ومع توظيف المكتبات الجامعية للتكنولوجيا الجديدة زادت فعالية وسرعة العمليات والإجراءات المكتبية، ويمكن تحديد فوائد إستخدام تكنولوجيا المعلومات في المكتبات في مجموعة من العناصر، وهي كمايلي:

- تجويد بيئة التعليم ووزيادة التفاعل بين عناصر عملية التعلم والتعليم.
- توفير بيئة تعليمية مناسبة لممارسة التفكير الإبداعي.
- توفير سبل البحث في قواعد البيانات وبنوك المعلومات.
- قابلية التعامل مع عدد كبير من المعلومات والخبراء[2]

2.5 دور المكتبات الجامعية

[1]. ميدون، ليلى. **تكنولوجيا المعلومات وتطبيقاتها في المكتبات الجامعية**.مجلة قبس للدراسات الإنسانية والإجتماعية. المجلد 06، العدد 02، 2022.ص978

[2]. المدادحة، أحمد نافع. **المكتبات الجامعية ودورها في عصر المعلومات**. عمان: مكتبة المجتمع العربي، 2004.ص100

تعد المكتبات الجامعية أحد المكونات الأساسية في المؤسسات العلمية، إذ تؤدي دور محوري في خدمة المؤسسات الجامعية والعملية التعليمة وخدمة المجتمع، وتتجل دور المكتبات الجامعية في عدة جوانب متكاملة، من أبرزها مايلي:

1.2.5 دور المكتبة الجامعية في دعم المنهج التعليمي

تتجل رسالة المكتبة التعليمية في مساندة ودعم المناهج العلمية من خلال تنمية قدرات الطالب في البحث عن المعلومات بهدف دعم التعليم الذاتي، فالنشاط التعليمي الذي يقوم به نتيجة رغبته الذاتية، بهدف صقل المعرفة وتنمية القدرات والمهارات لإستعاب معطيات العصر والتكيف معه.

فالمكتبات الجامعية حاليا تضم مجموعة من الأساليب التربوية التي تعزز كل من التعلم الذاتي والبناء الاجتماعي[1]. وعليه نجد أن المكتبة الجامعية تخطت فكرت أنها مجرد مركز للموارد الرقمية وأدوارها محدودة في مجموعة العمليات الإدارية والفنية، إذ ثبتت وجودها كوحدة متكاملة قوامها؛ البحث والتوجيه والإتصال حتى تتوافق مع جميع التغيرات المستجدة.

كما تؤدي المكتبات الجامعية دور هام في تعزيز البحث العلمي معتمدة في ذلك على خبرات وإمكانات ومهارات الموارد البشرية المؤهلة، وكمية ونوعية مصادر المعلومات التي تضمها الوسائل الإعلامية التي تستخدمها في خدمة أهداف الجامعة وجمهور المستفيدين. فالبحث العلمي يحتاج إلى معلومات وينتج معلومات جديدة وفي هذا الإطار يتوجب وجود مؤسسة تعنى بتوفير المعلومات التي يحتاجها الباحث لغرض الإفادة منها في البحوث المستقبلية[2] .

كما تسهم المكتبات الجامعية في دعم وتطوير العملية التعليمية في الجامعة من خلال مجموعة من المهام والوظائف الهامة، وأبرز هذه الوظائف مايلي:

- التعريف بمحتويات المكتبة من خلال القيام بمعارض وندوات وإصدار البيبليوغرافيات والمنشورات الخاصة بها، قصد التعريف بها وتنشيط الحركة العلمية وتوضيح كيفية التعامل والوصول إلى المقتنيات بسرعة ودقة.
- توفير المقتنيات وإتاحة الوصول إلى المعلومات على إختلاف أوعيتها سواء كانت تقليدية مثل: الكتب، المجلات، المخطوطات، النشرات، الرسائل والأطروحات الجامعية أو موارد رقمية.

---

[1]. عواد، مايا حفيظ. **التحول الرقمي في المكتبات الجامعية: إستخدام التقنيات الحديثة لتطوير المناهج التعليمية**. المجلة العربية للنشر العلمي. العدد الثامن والسبعون، 2025. ص835

[2]. بن عميرة، عبد الكريم. **سبل التعاون بين المكتبات جزائرية في العصر الرقمي وتوظيفها في العملية التعليمية: دراسة نظرية**. مجلة الأمير عبد القادر للعلوم الإسلامية. المجلد 36، العدد 02، 2022.ص 255

- توفر المكتبات الجامعية خدمة الإشتراك في العديد من قواعد البيانات والمجلات العلمية العالمية، إضافة إلى إنشاء مستودعات مؤسساتية للإطلاع على جميع الدراسات والأبحاث العلمية في مختلف التخصصات العلمية[1].
- تسع المكتبات الجامعية إل إستقطاب الرواد والباحثين وتوفير فضاءات بحثية مريحة وهادئة مخصصة للبحث العلمي سواء في العمل الفردي أو الجماعي بين الباحثين والطلبة، وإكسابهم الذاتية في البحث عن المعلومات.
- تساهم المكتبات الجامعية في شرح طرق التعامل ووالإستخدام للأدوات والتقنيات الحديثة التي تستخدمها المكتبة من أجل دعم وتطوير مهارات الباحثين والطلبة عن طريق تنظيم ورشات تدريبية وبرامج تكوينية[2].

3.5خدمات المكتبات الجامعية

تقدم المكتبات الجامعية مجموعة من الخدمات الموجهة للطلبة والباحثين بهدف دعم البحث العلمي وتعزيز قدراتهم للوصول إلى المعلومات المطلوبة، وتتفق جميع المكتبات الجامعية الجزائرية في توفير هذه الخدمات بإعتبارها خدمات قاعدية. وتتمثل خدمات المكتبات الجامعية الجزائرية في مايلي:

1.3.5 خدمة البحث المباشر في الفهرس الآلي:

البحث بالإتصال المباشر أو البحث البيبليوغرافي المباشر وهي خدمة تقدمها المكتبات على شبكة الأنترنت حيث يسمح للمستفيد بإدخال موضوع بحثه في فضاء مخصص للبحث متصل بقاعدة بيانات النظام، تتم هذه الخدمة في الفضاء السيبيراني ودون الحضور الفيزيائي للباحث للمكتبة.

توفر الخدمة للمستفيدين خدمات بيبليوغرافية ممثلة في قوائم بالمصادر التي تتطابق مع موضوع البحث سواء كان الوعاء على مستوى المكتبة أو المكتبات المتكتلة[1].

---

[1]. بوزارة، أحلام. **تعزيز مرئية الجامعات الجزائرية من خلال المكتبات الجامعية: دراسة حالة المكتبات المركزية في جامعة جيلالي اليابس سيدي بلعباس وجامعة فرحات عباس سطيف 1**. المجلة المغاربية للدراسات التاريخية. المجلد، 16. العدد،02، 2024.ص293-294

[2]. الزاحي، سمية. **مكانة المكتبات الجامعية في سياسة التعليم العالي في الجزائر: دراسة ميدانية بجامعة منتوري قسنطينة، عنابة وسكيكدة**. أطروحة دكتوراه. قسنطينة: جامعة منتوري، 2014.ص 124

2.3.5 خدمة تدريب المستفيدين

تحضى خدمة تدريب المستفيدينبإهتمام كبير في بيئة المكتبات، وهي: تدريب المستفيدين على كيفية إستخدام المصادر والخدمات المتعددة التي تقدمها المكتبات.وتشمل هذه الخدمة مجموعة من الأنشطة بهدف التعريف وتوعية المستفيدين وأيضا تدريبهم على كيفية إسخدام موارد المكتبة التقليدية والموارد الرقمية. وأدوات البحث والفهارس والكشافات،

تمثل خدمة تدريب المستفيدين الثمرة التي تقدمها المكتبات نتيجة تفاعل عناصر المدخلات، ذلك أن المستفيدين هم حجر أساس أي تخطيط أو تطوير لخدمات المعلومات، وبقدر ما تستطيع هذه الأخير من تلبية احتياجاهتم ترافقنجاح المكتبة وتطوره وإستمراريتها.ومما سبق يمكن تعريف خدمة تدريب المستفيدين بأنها: مجموعة الأنشطة والفعاليات المبرمجة والممنهجة من قبل المكتباتتهدف إلى تنمية المهارات الأساسية للمستفيدين وتزويدهم بالمعارف.والخبراتللإفادة من مصادر المعلومات وخدمات المعلومات المقدمة[2]

ولتحقيق هذه الغايات تقوم المكتبات الجامعية بمجموعة من الأنشطة، وهي كمايلي:

- إعداد اللوحات الإرشادية المناسبةلمكان المكتبة، مبانيها ومواردها.
- إعداد المطويات حول المكتبة ومجموعاتها وخدمات المعلومات المقدمة.
- إعداد الكتيبات والموجزات الإرشادية[3].

3.3.5 خدمة الإحاطة الجارية

---

[1]. **فوغالية**، صربينة. **واقع انضمام المكتبة الجزائرية الى الفهرس العربي الموحد ومساهمتها من خالله في ارلساء نظام معلومات عربي: درالسة ميدانية بالمكتبة الوطنية الجزائرية ومكتبة جامعة الجزائر 3**. مذكرة ماجستير، تختصص: المعلومات الإلكترونية: الإفتراضية وإستراتيجية البحث عن المعلومات، جامعة منتوري، قسنطينة.ص 164

[2]رايس، شيماء. **شبكات التواصل الاجتماعي ودورها في ترقية خدمات المعلومات بالمكتبات الرئيسية للمطالعة العمومية الجزائرية: دراسة تحليلية. أطروحة دكتوراه**. تخصص: علم المكتبات.عنابة: جامعة باجي مختار، 2021. ص94

[3]رايس، شيماء. **المرجع السابق**. ص94

تعرف خدمة الإحاطة الجارية بأنها إحاطة المستفيدين بكل ما يستجد من أوعية معلومات جديدة وصلت حديثة إلى المكتبة خلال عملية الإقتناء، وقد تتجاوز هذا المفهوم إلى إحاطة المستفيد بكل ما يستجد من أنشطة المكتب وبرامجها. وتعتبر خدمة الإحاطة الجارية من خدمات المعلومات المهمة وهي عملية إستعراض المعلومات المختلفة بأشكالها الورقية والإلكترونية ذات الصلة بإحتياجات المستفيدين، لتقديم الخدمة تتبع المكتبات الجامعية طرف وأساليب عديدة نذكر منها: البث الإنتقائي للمعلومات، النشرات، لوحة الإعلانات وتنظيم المعارض[1].

4.3.5 الخدمة المرجعية

تعد الخدمة المرجعية من أهم الخدمات المباشرة التي تقدمها المكتبات ومراكز المعلومات، والمعروف أن كل مكتبة مهما كان حجمها تضم قسم خاص بالمراجع أو قسم دوائر المعرفة، ويعرف **وليم كانز** الخدمة المرجعية بأنها:" عملية الإجابة عل الأسئلة بالإعتماد علة العناصر الثلاثة: المعلومات، المستفيد، أمين المراجع"[2]، إلا أن هذه العملية ليست بهذه البساطة في ظل التطورات السريعة لتكنولوجيا المعلومات وتعقد إحتياجات المستفيدين .

وفي ضوء ما سبق، نجد أن المكتبات الجامعية بيئة ديناميكية وملاذ كل باحث عن المعلومة، ولقد تم الإشارة إل مجموعة من الأدوار والخدمات التي تقدمها في المؤسسات الجامعية، إلا أن هذا لا يقلص أدوار المكتب ولا الخدمات المقدمة. فنجد خدمة الإعارة الخارجية، وخدمة الرد عل الإستفسارات وخدمة الإشتراك في الموارد الرقمية، خدمة إدارة الحجوزات ومع توجه المكتبات الجامعية نحو التعلم المفتوح بإستخدام تقنية RFIDتم إستحداث خدمات المعلومات بما يتلائم مع التقنية

4.5 مخطط الدراسة الإستطلاعية

تعد الدراسات الإستطلاعية البنة الأولى التي ترتكز عليها الدراسات البحثية في المراحل الأولى من إنجاز أي بحث علمي بهدف توضيح المعالم الأساسية للظاهرة المدروسة، كما أنها حلقة وصل بين الباحث والواقع المراد دراسته. حيث تتلاقى فيه ذهنية الباحث مع جوانب الموضوع ومعطياته، وللتفصيل في مجريات الدراسة الإستطلاعية قام الباحث بإعداد مخطط للدراسة تشمل مجموعة من العناصر.

1.4.5تعريف الدراسة الإستطلاعية

---

[1]. حمودي، سارة. **الخبرات المهنية للعاملين بالمكتبات الجامعية ودورها في تطوير الخدمات: من أجل توصيف المهام بمكتبة جامعة الجزائر 1**. مجلة دراسات وأبحاث. العدد 25، 2016،ص05

[2]. كوار، فوزية. **الخدمة المرجعية في المكتبات الجامعية الجزائرية**. مجلة الحضارة الإسلامية. المجلد، 1، العدد 28، 2016.ص.626

تعتبر الدراسة الإستطلاعية مرحلة مهمة في البحث العلمي؛وذلك لإرتباطها بالجانب التطبيقي فهي تسمح للباحث الحصول على معلومات أولية حول موضوع بحثه؛ ومن خلالها يمكن إنتقاء عينة الدراسة، وتوفر للباحث تقويم مناسبة للبيانات المتحصل عليها والتأكد من صلاحية الأدوات المستخدمة في الدراسة.

وتمثل الدراسة الإستطلاعية دراسة علمية مصغرة حول أثر خوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات المركزية عينة الدراسة وفق مبادئ حوكمة المعلومات ومبادئ مخاطر الأمن السيبراني وأيضا الوقوف على وعي إختصاصي المعلومات ومبادئها وأطرها وسياساتها.

2.4.5 أهداف الدراسة الاستطلاعية:

تم إجراء الدراسة الاستطلاعية خلال شهر مارس عام 2023 على عينة تجريبية من المجتمع الأصلي للدراسة.بلغ عددهم: 30 موظف بالمكتبات المركزية مختصين في علم المكتبات والمعلومات. موزعين على 04مكتبات مركزية بجامعات الشرق الجزائري (جامعة بسكرة؛ جامعة خنشلة؛ جامعة الوادي؛ جامعة باتنة2)، وعليه تم إعداد إستمارة تجريبية وتوزيعها على العينة الإستطلاعية.

يهدف الباحث من خلال الدراسة إلى إيجاد إجابات عن مجموعة تساؤلات محورية تتعلق بمراحل البحث العلمي المراد إنجازه، وتتحدد في العناصر التالية:

- التحقق من الخصائص السيكو مترية لأدوات الدراسة.
- التأكد من فهم العينة لمفردات أدوات الدراسة.
- إختبار صدق وثبات أداة جمع البيانات الرئيسية؛ إستمارة الإستبانة.
- التأكد من إمكانية إجراء الدراسة الميدانية.
- التعرف على الصعوبات التي يمكن أن تعترضنا قبل الدراسة الأساسية.
- الإطلاع على المادة العلمية والدراسات السابقة التي ناقشت متغير حوكمة المعلومات؛ ومتغير مخاطر الأمن السيبراني.
- البحث على نماذج من المقاييس المبنية في متغيرات الدراسة من أجل تحديد أهم المؤشرات التي يمكن إعتمادها في بناء وتطوير أدوات الدراسة.
- الحصول على وثائق إدارية من مديريات الجامعات(خلية الجودة؛خليةالرقمنة)، حول: برامج الحوكمة والإجراءات والسياسات الموثقة والمعتمدة في الأمن السيبراني وكذا التقييم الذاتي للمؤسسات المعنية .
- الحصول على إحصائيات من المكتبات المركزية للجامعات المعنية؛ عدد الموظفين؛ التجهيزات والبرامج.
- الإتصال بمحافظي المكتبات المركزية بهدف تحكيم حول: برامج حوكمة المعلومات ومخاطر الأمن السيبراني

- بعد الموافقة تم إرسال نسخ من أدوات الدراسة في صورتها الأولية من أجل تحكيمها.
- إسترجاع نسخ من أدوات الدراسة بعد تحكيمها من طرف أساتذة متخصيين، ثم إضافة التعديلات المقترحة من أجل إخراج أداة البحث في صورتها النهائية.

3.4.5 عينة الدراسة الاستطلاعية:

ثم تحديد عينة الدراسة الإستطلاعية خارج عينة الدراسة الأساسية من أجل توزيع أداة الدراسة بعد تحكيمها من طرف الاساتذة المحكمين وحساب الخصائص السيكو مترية (الصدق والثبات) والتأكد من مصداقية أدوات الدراسة وملائمتها مع المجال الجغرافي للدراسة والعينة.

شملت العينة الإستطلاعية (30) إختصاصي معلومات موزعين على أربع (04) جامعات بالشرق الجزائري ممثلة في:جامعة بسكرة، جامعة خنشلة، جامعة الوادي؛ وجامعة باتنة2. تم إختيار العينة المختارة بشكل عشوائي من مجتمع الدراسة وتم توزيعهم حسب الرتبة التالية:

02 رئيس محافظي المكتبات الجامعية.

02 محافظ المكتبات الجامعية.

08 ملحق بالمكتبات الجامعية من المستوى الاول.

07 ملحق بالمكتبات الجامعية من المستوى الثاني.

11 مساعد بالمكتبات الجامعية.

4.4.5 أداة جمع البيانات؛ البناء والتصميم

إعتمد الباحث في الدراسة الإستطلاعية على الإستبيان كأداة جمع البيانات، الهدف منه قياس أثر حوكمة المعلومات بأبعادها المسؤولية والإمتثال؛ الحفظ والإستبعاد على مخاطر الأمن السيبرانيبأبعاده السرية والسلامة التوافر.

1.4.4.5 تصميم أداة جمع البيانات:

تم تصميم إستبيان إلكتروني بالإعتماد على نموذج Google form، حيث تم تطبيق مقياس ليكارت الخماسي لقياس وجهات نظر العينة المبحوثة في كل عبارة،ومقياس ليكرت الخماسي مناسب للدراسات التي تعتمد على إستراتيجيات لقياس وجهات نظر وآراء الآخرين حول موضوع معين.

تم تقسيم الإستبيان إلى أربع (04) محاور رئيسية؛ يحتوي كل محور على مجموعة من الأسئلة على النحو التالي:

- **محور البيانات الشخصية.**

المحور الأول: وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني.

المحور الثاني:حوكمة المعلومات.

المحور الثالث: مخاطر الأمن السيبراني.

المحور الرابع: أثر حوكمة المعلومات على مخاطر الأمن السيبراني.

5.5 إجراءات الدراسة الإستطلاعية

1.5.5 الخصائص السيكو مترية لأداة جمع البيانات

يهدف البحث إلى تحديد أثر حوكمة المعلومات على مخاطر الأمن السيبرانيمن وجهة نظر أخصائي المعلوماتبمكتبات جامعات الشرق الجزائري، تم إعداد إستمارة بحث مقسمة إلى محاور؛يشمل كل محور مجموعة من المؤشرات للتحقيق في فرضية معينة،وتم توزيع الإستبيان على عينة بلغت(30) أخصائي المعلومات،تم الإختيار بشكل عشوائي من مجتمع الدراسة لتحقيق أهداف الدراسة الإستطلاعية.

1- صدق الأداة:

يعد الصدق من الشروط المهمة الواجب توافرها في أداة جمع البيانات، ويقصد بالصدق صلاحية الأسلوب أو الأداة لقياس ما هو مراد قياسهوبالتالي إرتفاع مستوى الثقة، فيما توصل إليه الباحث من نتائج يمكن تعميمهاتكون الأداة صادقة إذا حققت الغرض المطلوب والأداة الصادقة هي التي تستطيع قياس ما وضعت لقياسه .

قام الباحث بالتأكد من صدق الاستبانة بطريقتين:

أ.صدق المحكمين"الصدق الظاهري":

عرض الباحث الإستبانة على مجموعة من المحكمين تألفت من (04) متخصصين في علم المكتبات والتوثيق و(03) متخصصين في التسيير والإدارة من داخل الجامعات الجزائرية كما هو موضح في (**الملحق رقم 01**)،تم تقديم ملاحظات حول الأداة ومدى تلائم عبارات الأداة مع المحاور،تم الوقوف على الصياغة اللغوية للأداة، ومدى فهم المبحوثين للعبارات بالرجوع لملاحظات المحكمين تم إضافة وتعديل وحذف بعض العبارات للأداة، وضبط إستمارة الإستبيان بصورتها النهائية كما هو موضح في (**الملحق رقم 02**).

قام الباحث بحساب نسبة صدق المحتوى للأداة باستعمال معادلة (Lawshe)وهي كالتالي:

$$CVR= n-i/N$$

حيث:

- CVR: هو نسبة صدق المحتوى.

- n: هو عدد المحكمين الذين يعتبرون البند أساسي أو مهم.
- I: هو عدد المحكمين الذين يعتبرون البند ليس له صلة بالموضوع.
- N: هو مجموع المحكمين.

أظهرت نتائج المعادلة الإحصائية أن معامل إتفاق المحكمين على مدى صلاحية كل عبارة من عبارات الاستبيان تتراوح بين (0.71و1) كما هو موضح في (**الملحق رقم 03**)كما أن معامل الإتفاق للإستمارة لإستمارة حصل على معامل اتفاق (0.70) وهو مقبول.

جدول رقم (06):يوضح نسبة الاتفاق بين المحكمين

نسبة الاتفاق بين المحكمين	مستوى التقيم
80% الى 100%	مقبول
70% الى اقل من80%	تعدل
اقل من70%	تحذف

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

بالرغم من أن نسبة الإتفاق بين المحكمين كانت محصورة بين 70% الى 100%إلا أن بعض ملاحظات المحكمين جاءت بتعديل صياغة العبارات مع الإحتفاظ بالمعنى؛ تم تعديل العبارات إستنادا لتوجيهاتهم؛ وبذلك خرج الإستبيان في صورته النهائية، كما يوضح (**الملحق رقم 02**).

أ- صدق الإتساق الداخلي InternalValidity:

يقصد بصدق الإتساق الداخلي مدى اتساق كل فقرة من فقرات الإستبانة مع المحور الذي تنتمي إليه هذه الفقرة، قام الباحث بحساب الإتساق الداخلي للإستبانة وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات محاور الاستبانة والدرجة الكلية للمحور نفسه.

جدول رقم (07): معامل الإرتباط بين كل فقرة من فقرات المحور الاول "الوعي" والدرجة الكلية للمحور

		الفقرات	معامل بيرسون للارتباط	القيمة الاحتمالية(sig.)
المحور الاول: وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني	1	فهم المسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني.	0,790**	*0.000
	2	الفهم المشترك للمسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الامن السيبراني.	0,448*	*0.001
	3	التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الامن السيبراني.	0,489**	*0.006
	4	السياسات والإجراءات المتبعة في المكتبة تضمن حماية المعلومات.	0,007	*0.009
	5	الإطلاع بالشكل الكافي على الالتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة	0,790**	*0.000
	6	أخصائي المعلومات ملتزمون بتطبيق السياسات والإجراءات المتعلقة بأمن المعلومات.	0,448*	*0.001
	7	إدراك اهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات لمخاطر الامن السيبراني.	0,790**	*0.000
	8	الدراية بالإجراءات وتقنيات الحفظ التي يجب اتباعها واستخدامها لحفظ المعلومات بطريقة امنة ينجح حوكمة المعلومات لمخاطر الامن السيبراني.	0,448*	*0.001
	9	إدراك أهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات لمخاطر الامن السيبراني.	0,489**	*0.006
	10	الدراية بالإجراءات وتقنيات الحفظ التي يجب اتباعها واستخدامها لحفظ المعلومات بطريقة امنة ينجح حوكمة	0,790**	*0.000

		المعلومات لمخاطر الامن السيبراني.		

المصدر:من إعداد الطالب بالاعتماد على مخرجاتSPSS

نتائج الإتساق الداخلي للمحور الأول:" وعي أخصائي المعلومات بمفهوم حوكمة المعلومات لمخاطر الأمن السيبراني".

يوضح الجدول رقم (07) معامل الإرتباط بين كل فقرة من فقرات المحور الأول "الوعي" والدرجة الكلية للمحور؛ والذي يبين أن معاملات الإرتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$وبذلك يعتبر المحور صادق لما وضع لقياسه.

جدول رقم (08): معامل الارتباط بين كل فقرة من فقرات المحور الثاني "مستوى حوكمة المعلومات" والدرجة الكلية للمحور

		أولا: المـــــــسؤولية	معامل بيرسون للارتباط	القيمة الاحتمالية(sig.)
المحور الثاني:حوكمة المعلومات	11	توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة.	0,528**	*0.003
	12	تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات فيالمكتبة.	0,214	0,255غير دال
	13	تم تحديد المسؤوليات لحفظ وحذف المعلومات.	0,423*	*0.002
	14	هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين.	0,430*	*0.001
	15	يتم تنظيم دورات تدريبية متنوعة (تمكين العاملين)	0,554**	*0.001
	16	تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان التزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والامتثال للمعايير والسياسات.	0,490**	*0.06

ثـــــانيا:الامتـــــــثال			
17	تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية	0,805**	*0.000
18	يتم تنفيذ إجراءات الامتثال والتدقيق للتحقق من الامتثال للمعايير الداخلية والخارجية	0,386*	*0.003
19	تتبنى المكتبة استراتيجية لإدارة مخاطر عدم الامتثال	0,805**	*0.000
20	توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الامتثال وتوضيح المعايير والممارسات المطلوبة	0,484**	*0.007
21	يتم اجراء مراجعات دورية للتحقق من مدى الامتثال	0,805**	*0.000
22	تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية	0,484**	*0.007
ثـالثـــا:الحـــــــــفظ			
23	تلتزم المكتبة بمبدأ الحفاظ على المعلومات للفترة الزمنية اللازمة وفقًا للمتطلبات القانونية والتنظيمية	0,731**	*0.000
24	تستخدم المكتبة (الوسائل ؛ مواد؛ برمجيات)للحفظ الامن؛وارشفة المعلومات	0,533**	*0.002
25	تتبع المكتبة سياسات واجراءات لحفظ المعلومات والحفاظ على سلامتها واستمراريتها وبشكل صحيح ومنظم	0,731**	*0.000
26	تتم مراجعة وتحديث سياسات حفظ المعلومات بانتظام وفقا للمتطلبات القانونية والتنظيمية	0,533**	*0.002

	والتشغيلية.		
27	تستخدم المكتبة تقنيات الارشفة الملائمة للمحافظة على المعلومات بشكل دائم	0,362*	*0.005
28	تطبق المكتبة إجراءات النسخ الاحتياطي الدوري واختبار الاسترجاع لضمان استمرارية المعلومات وإتاحتها عند الحاجة.	0,393**	*0.006
رابـــــــــعا:الاستـــــــبعاد			
29	يتم استبعاد المعلومات بشكل منتظم وفقا للسياسات والمتطلبات القانونية	0,658**	*0.000
30	يتم الإستبعاد تلقائيا للمعلومات المخزنة الكترونيا بشكل نهائي من الفهارس	0,572**	*0.001
31	تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات	0,658**	*0.000
32	توفر المكتبة برامج للتوعية والتدريب المستمر بشأن ترتيبات المصير النهائي للمعلومات	0,572**	*0.001
33	توثق المكتبة جميع الاجراءات المتعلقة بترتيبات المصير النهائي للمعلومات	0,384*	*0.003
34	يتم تقييم مدى إلتزام المكتبة بسياسات الاستبعاد وتحسين فعالية الاجراءات المتبعة.	0,194**	*0.003

* **المصدر**: من إعداد الباحث بالاعتماد على مخرجاتSPSS

نتائج الاتساق الداخلي للمحور الثاني " مستوى حوكمة المعلومات"

يوضح جدول رقم (08) عامل الارتباط بين كل فقرة من فقرات المحور الثاني "مستوى حوكمة المعلومات" والدرجة الكلية للمحور؛ والذي يبين معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المحور صادق لما وضع لقياسه.

جدول رقم (09): معامل الارتباط بين كل فقرة من فقرات المحور الثالث " مستوى مخاطر الامن السيبراني " والدرجة الكلية للمحور

		أولا: المخاطر المتعلقة بالسرية	معامل بيرسون للارتباط	القيمة الاحتمالية(sig.)
المحور الثالث : مخاطر الامن السيبراني	35	هجمات التنصت (اعتراض شبكة الاتصالات او التقاط البيانات اثناء نقلها داخل وخارج المكتبة).	0,420*	*0.002
	36	هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام او المنقولة عبر الشبكة).	0,656**	*0.000
	37	الوصول غير المصرح به لنظام المكتبة من قبل اطراف خارجية مثل المهاجمين	0,410*	*0.002
	38	الوصول غير المصرح به لنظام المكتبة من قبل اطراف داخلية مثل المكتبيين(الموظفين)	0,331	*0.007
	39	الافعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة).	0,355	*0.005
	40	الافعال المتعمدة المتعلقة بالابتزاز(الابتزاز بالكشف عن المعلومات).	0,441*	*0.001
	41	هجمات الاصطياد الالكتروني؛ انتحال هوية اشخاص او منظمة يثق بهم الضحية باستخدام وسائل تقنية.	0,420*	*0.002
	42	هجمات الهندسة الاجتماعية (القدرة على التمثيل	0,656**	*0.000

	واقناع الضحية بالإفصاح عن المعلومات السرية).		
ثـــــــانيا:المخاطر المتعلقة بالسلامة			
43	الادخال الغير متعمد للبيانات الخاطئة من قبل الموظفين	0,682**	*0.000
44	اتلاف البيانات غير متعمد من قبل الموظفين	0,349	*0.005
45	اتلاف البيانات المتعمد من قبل الموظفين	0,682**	*0.000
46	الادخال المتعمد للبيانات الخاطئة من قبل الموظفين .	0,445*	*0.001
47	اخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين اثناء كتابة البرامج.	0,226	,231
48	التقادم التكنولوجي مثل الاجهزة والانظمة المتقادمة.	0,580**	*0.001
ثـالثـــا:المخاطر المتعلقة بالتوافر			
49	هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول الى الخدمة).	0,658**	*0.000
50	تفجير البريد الالكتروني (اغراق بريد المكتبة بالرسائل مما يؤدي الى توقفه عن العمل).	0,572**	*0.001
51	الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف.	0,194	*0.003
52	اعطال اجهزة النظام الفنية.	0,572**	*0.001
53	اعطال معدات الشبكة الفنية.	0,384*	*0.003

54	انقطاع شبكة الإنترنت أو ضعف الاتصال بالشبكة بما يؤثر على إتاحة الخدمات الرقمية واستمراريتها.	0,658**	*0.000
رابـــــــــعا:المخـــــاطر العـــــــــــامة			
55	قرصنة الهاتف (اجراء مكالمات مجانية؛ او الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .)	0,417*	*0.002
56	هجمات الانتحال مثل انتحال عنوانIP؛ او البريد الالكتروني؛ او موقع الويب؛ او هوية المتصل.	0,563**	*0.001
57	فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).	0,208*	0,270
58	ديدان الحاسوب(قادرة على استنساخ نفسها تلقائيا).	0,639**	*0.000
59	احصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله).	0,415*	*0.002
60	برامج التجسس الالكتروني(برامج خفية تراقب استخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم).	0,639**	*0.000
61	القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدا بتدمير المعلومات).	0,417*	*.0002
62	هجمات الرسائل المزعجة او الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل.	0,563**	*0.001

* **المصدر**: من إعداد الباحث بالاعتماد على مخرجاتSPSS

نتائج الإتساق الداخلي لمحور الثالث " مستوى مخاطر الامن السيبراني"

يوضح جدول رقم (09) عامل الارتباط بين كل فقرة من فقرات المحور الثالث "مخاطر الامن السيبراني" والدرجة الكلية للمحور؛ والذي يبين معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$وبذلك يعتبر المحور صادق لما وضع لقياسه.

جدول رقم (10): معامل الارتباط بين كل فقرة من فقرات المحور الرابع"اثر حوكمة المعلومات على مخاطر الامن السيبراني"والدرجة الكلية للمحور

		أولا وضوح السياسات الداخلية ومسؤوليات الأفراد فيما يتعلق بإدارة البيانات الحساسة. (إدارة إطار الحوكمةCOBIT 5: APO01)؛ ISO 27001 A.6(تنظيم أمن المعلومات)	معامل بيرسون للارتباط	القيمة الاحتمالية(sig.)
المحور الرابع : اثر حوكمة المعلومات على مخاطر الامن السيبراني	63	عندما تكون المسؤوليات موزعة بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة. هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به، حيث يتم تطبيق تدابير تحكمية دقيقة تحد من عدد الأشخاص الذين لديهم إمكانية الوصول إلى البيانات الحساسة.	0,880**	*0.000
	64	توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها. هذا يسهم في تعزيز سلامة البيانات، حيث أن كل عملية تعديل تُراجع وتُعتمد من قبل المسؤولين المعنيين.	0,414**	*0.002
	65	وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام	0,866**	*0.000

	بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية.		
ثـــــانيا: تكامل سياسات المكتبة مع التشريعات والمعايير العالمية للأمن السيبراني. COBIT 5: MEA03 ضمان الامتثال)؛(ISO 27001: A.18 الامتثال)؛(الامتثال وإدارة المخاطر ITIL)			
66	الامتثال للقوانين والتشريعات مثل GDPR وغيرها من المعايير العالمية يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة، ما يقلل من فرص التسريب أو الاختراق.	0,374*	*0.004
67	الامتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية مثل التشفير، التحقق متعدد العوامل، والتحديثات الأمنية الدورية، مما يحافظ على سلامة البيانات ويمنع التلاعب بها.	0,907**	*0.000
68	تتطلب التشريعات غالبًا خططًا للطوارئ واستمرارية الأعمال. الامتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الانقطاع غير المخطط له.	0,907**	*0.000
ثـالثـــا: كفاءة نظام إدارة دورة حياة البيانات . () COBIT 5: DSS06 إدارة استمرارية الأعمال)؛ ISO 27001: A.8 (إدارة الأصول)			
69	تطبيق سياسات الحفظ السليمة يضمن أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للاختراقات.	0,635**	*0.000
	سياسات الحفظ التي تشمل عمليات مراجعة وتدقيق دورية تساهم في الحفاظ على سلامة	0,643**	*0.000

70	البيانات، حيث تتيح التعرف على أي تغييرات غير مصرح بها أو تلف قد يحدث للبيانات على المدى الطويل.		
71	ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة التي قد تعيق الوصول الفعّال إلى المعلومات الهامة، مما يحسن من توافر البيانات الضرورية.	0,478**	*0.007
	رابـــــــــعا:فعالية وأمان عمليات استبعاد البيانات الحساسة.		
	(COBIT 5: DSS06 (إدارة استمرارية الأعمال) DSS02إدارة خدمة الأمن(؛) ISO 27001: A.8إدارة الأصول) و) A.11التحكم في الوصول(؛)ITILإدارة الطلب والحوادث		
72	إجراءات الاستبعاد المطبقة بشكل صحيح تضمن أن البيانات الحساسة لا يمكن استعادتها بعد الحذف، مما يحميها من الاستخدام غير المشروع ويضمن بقاء المعلومات الخاصة تحت السيطرة الكاملة.	0,686**	*0.000
73	تنفيذ عمليات الاستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية.	0,484**	*0.007
74	الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة.	0,644**	*0.000

* **المصدر**: من إعداد الباحث بالاعتماد على مخرجاتSPSS

نتائج الاتساق الداخلي للمحور الرابع"أثر حوكمة المعلومات على مخاطر الامن السيبراني"

يوضح الجدول رقم (10) عامل الارتباط بين كل فقرة من فقرات الرابع "أثر حوكمة المعلومات على مخاطر الامن السيبراني"والدرجة الكلية للمحور؛ والذي يبين معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$وبذلك يعتبر المحور صادق لما وضع لقياسه.

2.الصدق البنائي Structure Validity

يعتبر الصدق البنائي أحد مقاييس صدق الأداة، بهدف إلى قياس مدي تحقق الأهداف التي تريد الأداة الوصول إليها؛ ويبين مدى إرتباط كل محور من محاور الدراسة بالدرجة الكلية لفقرات الاستبانة، كما يوضحه الجدول رقم :01

جدول رقم (11): معامل الارتباط بين درجة كل محور من محاور الاستبانة والدرجة الكلية للاستبانة.

الرقم	المحور	معامل بيرسون للارتباط	القيمة الاحتمالية(sig.)
01	وعي اخصائي المعلومات بحوكمة المعلومات لمخاطر الامن السيبراني.	0,891**	*.0000
02	مستوى حوكمة المعلومات	0,987**	*.0000
03	مستوى مخاطر الامن السيبراني	0,991**	*.0000
04	اثر حوكمة المعلومات على مخاطر الامن السيبراني	0,928**	*.0000

* **المصدر**: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يوضح نتائج أن جميع معاملات الإرتباط مرتفعة في جميع محاور الإستبانة دالة عند مستوى معنوية $\alpha \leq 0.05$حيث بلغت معاملات الإرتباط 0.891 لمحور وعي أخصائي المعلزمات بحوكمة المعلومات، وبلغ معامل الإرتباطمستوى حوكمة المعلومات 0.987، وبلغ معامل الإرتباط مستو مخاطر الأمن السيبراني 0.991، في حين بلغ معامل الإرتباط أثر حوكمة المعلومات 0.928 ، وكلها عند القيمة الإحتمالية Sig=0.000

وبذلك جميع محاور الإستبانة تتمتع بصدق بنائي مرتفع وأنها صادقة لما وضعت لقياسه،

3.ثبات الأداةReliability:

يشير مفهوم ثبات الأداة إلى مدى إتساق نتائج الأداة المستخدمة في جمع البيانات، أي مدى إمكانية الحصول على نفس النتائج إذا طبقنا أداة جمع بيانات نفسها عدة مرات على مفردات نفس العينة.

ولغرض التحقق من ثبات الإستقرار لأداة الدراسة،تم حساب قيمة معامل ثبات الاتساق الداخلي باستخدام معادلة الفا كرونباخCronbach's Alpha Coefficient(**انظر الملحق رقم04**)،حيث بلغ معامل الثبات(0.943)،وبالنظر لقيم معاملات الثبات يتضح أنها صالحة لإستخدامها من أجل تحقيق أهداف الدراسة ويمكن توضيح قيمة معامل الثبات الفا كرونباخ بشكل مفصل لكل محاور استبيان في الجدول الموالي:

جدول رقم (12):يوضح معامل الثبات الفا كرونباخ في محاور الاستبانة

المحور	عدد الفقرات	معامل الفا كرونباخ	الصدق الذاتي*
وعي اخصائي المعلومات بحوكمة المعلومات لمخاطر الامن السيبراني.	10	0,747	0.864
حوكمة المعلومات	24	0,799	0.894
مخاطر الامن السيبراني	28	0,853	0.924
أثر حوكمة المعلومات على مخاطر الامن السيبراني	12	0,668	0.817
الدرجة الكلية	74	0,943	0.971

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

***الصدق الذاتي = الجذر التربيعي الموجب لمعامل الفا كورنباخ**

يوضح الجدول رقم(12) أن قيمة معامل الفا كورنباخ مرتفعة لمحاور الإستبانة حيث تتراوح بين

(0.668-0.853)، بينما بلغت قيمة الثبات للدرجة الكلية لجميع فقرات الإستبانة (0.943). كما تظهر النتائج أن قيمة الصدق الذاتي مرتفعة لكل مجال حيث تتراوح بين(0.817-0.924) بينما بلغت الدرجة الكلية لجميع فقرات الإستبيان (0.911) وهو ما يدل عل أن معامل الصدق الذاتي مرتفع.

وعليه يكون الإستبيان في صورته النهائية كما يوضحه الملحق رقم (02) قابلة للتوزيع، ويكون الباحث قد تأكد من صدق وثبات أداة الدراسة وصلاحيتها بهدفالإجابة على أسئلة الدراسة وإختبار فرضياتها.

6.5 مخرجات الدراسة الإستطلاعية

بعد تطبيق أدوات الدراسة على أفراد العينة الاستطلاعية، توصلت الدراسة إلى ما يلي:

1. التحقق من الخصائص السيكومترية لأداة الدراسة (الصدق والثبات)، والتأكد من صلاحيتها للإستخدامها في الدراسة الأساسية.
2. التأكد من وضوح مفردات الإستبيان ومصطلحاته لدى أفراد العينة بما يضمن سلامة الفهم أثناء التطبيق الميداني.
3. إختبار صلاحية أداة الإستمارة للإستخدام في بيئة المكتبات الجامعية، تمهيدًا لاعتمادها في صورتها النهائية.
4. التأكد من إمكانية تنفيذ إجراءات الدراسة الميدانية (الإتاحة، الزمن، التعاون الإداري)، بما يضمن قابلية التطبيق العملي في الدراسة الأساسية.
5. إستباق الصعوبات التطبيقية المحتملة قبل الشروع في الدراسة الأساسية، بما يسمح بتعديل الإجراءات وتفادي العوائق أثناء التنفيذ.
6. إعتماد الأساليب الإحصائية المناسبة للتحقق من الصدق والثبات في الدراسة الاستطلاعية، وذلك بالاعتماد على:

- معامل ألفا كرونباخ لحساب الثبات.
- معامل ارتباط بيرسون لصدق الاتساق الداخلي.
- معامل الاتفاق (CVR) بمعادلة لاوشي لصدق المحكمين.
- معامل ارتباط بيرسون للصدق البنائي.

7. إخراج الاستبيان في صورته النهائية (**الملحق رقم 02**) بعد التأكد من صدقه وثباته وصلاحيته لتغطية أسئلة الدراسة وإختبار فرضياتها.
8. توثيق إجراءات الدراسة الاستطلاعية بما يدعم ضبط الدراسة الأساسية؛ إذ أُجريت خلال شهر مارس 2023 على عينة تجريبية (30) موزعة على أربع مكتبات مركزية بجامعات الشرق الجزائري (بسكرة، خنشلة، الوادي، باتنة 2.

1.6.5 الأساليب الإحصائية المستخدمة في الدراسة :

تم إستخدام برنامج التحليل الإحصائي في العلوم الاجتماعية (Spss22) لأجل تحليل نتائج الدراسة، وتمثلت الأدوات الإحصائية المستخدمة فيما يلي:

1.1.6.5 الدراسة الإستطلاعية :

- معامل الفا كرونباخ لحساب ثبات الإستبيان.
- معامل الإرتباط بيرسون لحساب صدق الإتساق الداخلي لمعرفة مدى ارتباط كل فقرة من فقرات بالمحور الذي تنتمي اليه.
- معامل الإتفاق CVR بمعادلة لاوشي لحساب الصدق الظاهري (صدق المحكمين) لأدوات الدراسة .
- معامل الإرتباط بيرسون لحساب الصدق البنائي لمعرفة مدى إرتباط كل محور من المحاور بالدرجة الكلية للاستبيان.

2.1.6.5الدراسة الأساسية:

- إختبار Shapiro-Wilk من أجل إختيار الأساليب الإحصائية المناسبة (الأساليب البارمترية، الأساليب اللابرامترية) لإختبار فرضيات الدراسة.
- . النسب المئوية والتكرارات.
- . المتوسطات الحسابية من أجل معرفة مستوى حوكمة المعلومات وكذا مستوى مخاطر الأمن السيبراني والحكم عليها ما إذا كانت مرتفعة او متوسطة؛ أو منخفضة.
- الإنحرافات المعيارية من أجل قياس الإختلاف بين درجات العينة ومقدار التشتت بينها.
- إختبار t.test لدلالة الفروق لحساب
- معادلة مربع ايتا (η^2) لحساب حجم أثر حوكمة المعلومات
- . معامل الإرتباط بيرسون.
- . المتوسط المرجع لمقياس ليكرت الخماسي.

يتم حسابهذا الأخير عن طريق حساب المدى،حيث يساوي(5-1=4) يرمز الرقم (5) لعدد خيارات مقياس ليكرت الخماسي (موافق بشدة ،موافق،محايد،غير موافق،غير موافق بشدة)، ثم حساب طول الفئة من خلال تقسيم المدى على عدد الفئات أي(4/5=0.80)فتكون الفئة الأولى لقيم المتوسط الحسابي من (1الى 1+0.80)، و القيمة الثانية تبدأ من المجال(1.81الى2.60). تم حساب قيمة (2.60)عن طريق إضافة(0.80)الناتجة عن تقسيم مدى الفئات إلى (1.80)وهكذا بالنسبة لبقية المتوسطات الحسابية.

والجدول الموالي يفسر طريقة تفسير قيم المتوسطات الحسابية:

الجدول رقم(13): يبين مستوى قيم المتوسط المرجع لمقياس ليكرت الخماسي:

المتوسط المرجح	المستوى
من 1 الى 1.80	منخفضة
من 1.81 الى 2.60	
من 2.61 الى 3.40	متوسطة
من 3.41 الى 4.20	مرتفعة
من 4.21 الى 5	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

خلاصة الفصل:

تعد الدراسات الإستطلاعية مرجعية الباحث في معالجة موضوع الدراسة، حيث يتسهم بدرجة كبيرة في تحديد مدى تطابق الموضوع مع الظاهرة المراد دراستها من الناحية الأدبية والجغرافية والبشرية. وإستناد الأدبيات على هذا النوع من الدراسات في مرحلة البحث وبناء الموضوع يرجع لدقة مخرجاتها.

إضافة إلى ذلك لدراسة الإستطلاعية تمثل دراسة مختصرة للدراسة الأساسية، وقاعدة أساسية في بناء وتصميم ومعالجة البحث النهائي.

الفصل السادس: وعي أخصائي المعلومات بأثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات الجامعية

تمهيد

خصص الإطار الميداني للدراسة؛ الفصل السادس في قياس مستوى وعي أخصائي المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري بموضوع حوكمة المعلومات ومخاطر الأمن السيبراني في ظل التوجهات الحديثة للمكتبات عينة الدراسة نحو التحول الرقمي، كما تحاول الدراسة قياس مستوى حوكمة المعلومات ومخاطر الأمن السيبراني في بيئة المكتبات والوقوف على أثر تطبيق حوكمة المعلومات للتقليل من التهديدات والمخاطر المحتملة في الفضاء السيبراني، وتحديد الفروقات ذات الدلالة الإحصائية لمتغيرات الدراسة.

1.6وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني في المكتبات الجامعية.

يعد وعي أخصائي المعلومات بحوكمة المعلومات أحد العوامل الأساسية في تعزيز الأمن السيبراني داخل المكتبات الجامعية، ذلك أن حوكمة المعلومات تساعد في وضع سياسات وإجراءات لإدارة البيانات وحمايتها وحفظها من المخاطر والتهديدات سواء كانت تهديدات بشرية أو تهديدات سيبرانية، وتطبيق أفضل الممارسات في إدارة المعلومات والنظم الآلية.

أولا: إختبار الفرضية الرئيسية الأولى.

" مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري متوسط "

يشمل المحور الأول؛ وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري على 10 عبارات تهدف من خلالها لمعرفة مستوى وعي أخصائي المعلومات بالمكتبات المركزية محل الدراسة بالموضوع، وسنقوم بعرض نتائج هذه العبارات في النقاط الموالية.

ثانيا: عرض وتحليل الفقرات المتعلقة بمستوى الوعي.

تم استخدام إختبارt للعينة الواحدة والنتائج مبينة في الجدول أدناه يبين آراء أفراد عينة الدراسة في فقرات"وعي أخصائي المعلومات لمخاطر الأمن السيبراني".

الجدول رقم (14): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المحور الاول "وعي اخصائي المعلومات"

وعي أخصائي المعلومات		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (Sig.)	درجة التبني	الترتيب
فهمالمسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني.	التكرار	26	44	7	25	8	2.50	1.276	-4.109	0.000	منخفضة	10
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
الفهمالمشترك بين أخصائي المعلومات لأهمية المسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الأمن السيبراني.	التكرار	14	47	16	27	6	2.67	1.142	-3.005	0.002	متوسطة	5
	الوزن النسبي	12.7	42.7	14.5	24.5	5.5						
التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الأمن السيبراني.	التكرار	14	43	11	30	12	2.85	1.265	-1.282	0.203	متوسطة	4
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
حوكمة المعلومات هي مجموعة السياسات والإجراءات التي تُطبق في المكتبات الجامعية لتنظيم وإدارة المعلومات بهدف تقليل وتعزيز الحماية ضد المخاطرالسيبرانية.	التكرار	25	37	11	29	8	2.62	1.292	-3.099	0.002	متوسطة	7
	الوزن النسبي	22.7	33.6	10	26.4	7.6						
مخاطر الأمن السيبرانيمن الناحية العملية على أنها التهديدات والثغرات المحتملة التي قد تؤثر سلبًا على سرية وسلامة وتوافر أنظمة المعلومات والبيانات داخل المكتبات الجامعية.	التكرار	20	32	10	28	20	2.96	1.420	-4.109	0.000	متوسطة	2
	الوزن النسبي	18.2	29.1	9.1	25.5	18.2						
الإطلاع بالشكل الكافي على الإلتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة	التكرار	7	28	47	16	12	2.98	1.049	-3.187	0.002	متوسطة	1
	الوزن النسبي	6.4	25.5	42.7	14.5	10.9						
السياسات والإجراءات المتبعة في المكتبة تضمن حماية المعلومات والإمتثال للمعايير القانونية والتنظيمية.	التكرار	25	42	7	27	9	2.57	1.302	-4.441	0.000	منخفضة	9
	الوزن النسبي	22.7	38.2	6.4	24.5	8.2						
أخصائي المعلومات ملتزمون بتطبيق السياسات والإجراءات المتعلقة بأمن المعلومات.	التكرار	14	48	16	26	6	2.65	1.137	-3.187	0.002	متوسطة	6
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
إدراك أهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة	التكرار	14	40	12	28	16	2.93	1.311	-1.282	0.203	متوسطة	3
	الوزن النسبي	12.7	36.4	10.9	25.5	14.5						

المعلومات لمخاطر الأمن السيبراني.											
الدراية بالإجراءات وتقنيات الحفظ التي يجب إتباعها وإستخدامها لحفظ المعلومات بطريقة آمنة ينجح حوكمة المعلومات لمخاطر الأمن السيبراني.	التكرار	25	40	8	28	9	2.60	1.308	-3.208	0.000	منخفضة	8
	الوزن النسبي	22.7	36.4	7.3	25.5	8.2						
مستوى وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني							2.73	0.60	-4.650	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تشير النتائج إلى أن المتوسط الحسابي العام لجميع فقرات المحور تساوي (2.73)، مع إنحراف معياري قدره (0.60)، مما يشير إلى عدم وجود تشتت كبير في الإجابات، وقيمة t تساوي -4.650 ووفقا لمقياس الدراسة يظهر أن الاتجاه العام لآراء المبحوثين حول هذا المحور كان متوسطا، مع قيمة إحتمالية دالة إحصائيًا عند

(Sig = 0.000)مما يدل على أن مستوى وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني متوسطة عند مستوى دلالة إحصائية 0.0 5 α.

يمكن تفسير هذه النتيجة من خلال تحليل الفقرات المتعلقة بقياس مستوى وعي أخصائي المعلومات، تم ترتيب فقرات هذا المحور وفقا لآراء المبحوثين ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة، مع ذكرها وتفسيرها:

1. الإطلاع بالشكل الكافي على الإلتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة.

رجع الباحث سبب الإرتفاع النسبي في نتيجة الفقرة: "الإطلاع بالشكل الكافي على الإلتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة". تمتع غالبية أخصائي المعلومات بوعي قانوني مقبول فيما يخص حوكمة المعلومات ويُعزى ذلك على الأرجح إلى تلقيهم تكوينًا قانونيًا، أو إلى التوجيهات الإدارية المستمرة داخل الجامعات محل الدراسة، مما ساهم في تعزيز إدراكهم لأهمية الإمتثال للإطار التشريعي والتنظيمي المتعلق بحماية المعلومات.

2. مخاطر الأمن السيبراني من الناحية العملية على أنها التهديدات والثغرات المحتملة التي قد تؤثر سلبًا على سرية وسلامة وتوافر أنظمة المعلومات والبيانات داخل المكتبات الجامعية.

تعكس نتيجة الفقرة: "مخاطر الأمن السيبراني من الناحية العملية على أنها التهديدات والثغرات المحتملة التي قد تؤثر سلبًا على سرية وسلامة وتوافر أنظمة المعلومات والبيانات داخل المكتبات الجامعية"، والتي سجلت متوسطًا حسابيًا قدره (2.96) على إهتمام المكتبات الجامعية محل الدراسة برفع مستوى وعي أخصائي المعلومات

بالمفاهيم الأساسية لمخاطر الأمن السيبراني، ما يعكس فهمًا مفاهيميًا وتقنيًا مقبولًا لأبعاد هذه المخاطر من حيث تأثيرها على سرية البيانات وسلامتها وتوافرها.

3. إدراك أهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات لمخاطر الأمن السيبراني.

تُظهر نتيجة الفقرة "إدراك أهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات لمخاطر الأمن السيبراني"، أن هناك وعيًا جيد بأهمية تأمين البيانات، خصوصًا من حيث التحكم في الوصول. ما يعكس إدراكًا واضحًا لدى هذه المكتبات لأحد المبادئ الجوهرية في حوكمة المعلومات لمخاطر الأمن السيبراني والمتمثل في مبدأ السري(Confidentiality) ، إلا أنه لا يكشف بالضرورة عن مستوى التطبيق العملي.

4. التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الامن السيبراني.

تدل نتيجة الفقرة:"التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الأمن السيبراني".على أن بعض المكتبات الجامعية تبذل جهودا في التكوين، إلا أن المتوسط المتوسط يشير أيضًا إلى وجود تفاوت واضح في الإستفادة أو التغطية. قد يرجع ذلك إلى ضعف البرامج التدريبية أو اقتصارها على جوانب نظرية دون دعم تقني عملي.

5. الفهم المشترك بين أخصائي المعلومات لأهمية المسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الأمن السيبراني.

تشير نتيجة هذه الفقرة " الفهم المشترك بين أخصائي المعلومات لأهمية المسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الأمن السيبراني"، إلى وجود وعي نسبي بأهمية التعاون والمسؤولية الجماعية لكنها لا تزال أقل من المتوقع في بيئة تعتمد على التنسيق بين مختلف الفاعلين، قد يعود ذلك إلى ثقافة مؤسسية تركز على المسؤولية الفردية أو غياب آليات العمل التشاركي.

6. أخصائي المعلومات ملتزمون بتطبيق السياسات والإجراءات المتعلقة بأمن المعلومات

تعكس نتيجة الفقرة "أخصائي المعلومات ملتزمون بتطبيق السياسات والإجراءات المتعلقة بأمن المعلومات."إلى ضعفًا نسبيًا في الإلتزام الفعلي رغم تأكيد أغلب المكتبات الجامعية بتوفر السياسات، ما يدل على فجوة بين

المعرفة والإمتثال الفعلي. قد تُعزى هذه النتيجة إلى غياب الرقابة أو ضعف التحفيز المؤسسي لتطبيق تلك السياسات.

7. حوكمة المعلومات هي مجموعة السياسات والإجراءات التي تُطبق في المكتبات الجامعية لتنظيم وإدارة المعلومات بهدف تقليل وتعزيز الحماية ضد المخاطر السيبرانية.

تُظهر نتيجة الفقرة " حوكمة المعلومات هي مجموعة السياسات والإجراءات التي تُطبق في المكتبات الجامعية لتنظيم وإدارة المعلومات بهدف تقليل وتعزيز الحماية ضد المخاطر السيبرانية"، أن المفهوم الشامل لحوكمة المعلومات لا يزال غامضًا لدى بعض المكتبين، رغم وجود وعي نسبي. وهذا يدل على حاجة ماسة إلى توضيح المفاهيم التنظيمية ضمن دورات التكوين.

8. الدراية بالإجراءات وتقنيات الحفظ التي يجب إتباعها وإستخدامها لحفظ المعلومات بطريقة آمنة ينجح حوكمة المعلومات لمخاطر الأمن السيبراني.

تشير نتيجة الفقرة " الدراية بالإجراءات وتقنيات الحفظ التي يجب إتباعها وإستخدامها لحفظ المعلومات بطريقة آمنة ينجح حوكمة المعلومات لمخاطر الأمن السيبراني" إلى ضعف المعرفة التقنية لدى المكتبين، وهو مؤشر خطير خاصةً في ظل التطورات والتغيرات التكنولوجية. هذا الأمر يتطلبضرورة برمجة تدريب تقني متخصص لتعزيز مهاراتهم في أدوات الحفظ والتشفير وأنظمة النسخ الاحتياطي وغيرها.

9. السياسات والإجراءات المتبعة في المكتبة تضمن حماية المعلومات والإمتثال للمعايير القانونية والتنظيمية.

تعكس نتيجة الفقرة " السياسات والإجراءات المتبعة في المكتبة تضمن حماية المعلومات والإمتثال للمعايير القانونية والتنظيمية" المنخفضة شكوكًا لدى المكتبين حول فعالية السياسات المعتمدة، أو ربما عدم إطلاعهم الكافي على السياسات والإجراءات في المؤسسة، كما يشير ذلك إلى ضعف التواصل الداخلي بالمكتبات محل الدراسة بشأن المعايير المعتمدة وضرورة مراجعة مدى فعاليتها أو وضوحها.

10.فهم المسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني.

تعد هذه الفقرة " فهم المسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني." الأضعف وعيًا، وهي تعكس قصورًا خطيرًا في إدراك المكتبين لدورهم الفردي في حوكمة

المعلومات لمخاطر الأمن السيبراني. يُفترض أن يكون كل مكتبي خط دفاع أول ضد المخاطر السيبرانية، لذا فإن ضعف هذا الفهم يشكل تحديًا مؤسسيًا واضحًا ويستوجب تدخلًا عاجلًا.

مما سبق نخلص إلى القول بأن نتائج عبارات المحور الأول "وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني" يتراوح بين المتوسط والضعيف، مع وعي قانوني ومفاهيمي مقبول، يقابله ضعف واضح في الفهم الفردي والتقني والتطبيقي. ويُستنتج أن هناك حاجة إلى تكوين تكميلي شامل يشمل الجوانب النظرية، الإجرائية، والتقنية لحوكمة المعلومات لمخاطر الأمن السيبراني.

2.6 مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري منخفض

يمثل مستوى تطبيق حوكمة المعلومات بالمكتبات الجامعية مؤشر هام على مدى إلتزام هذه المكتبات بالمعايير والإجراءات التي تكفل الإستخدام الآمن للمعلومات، ويتحدد مستوى تطبيقها في أي مؤسسة بمجموعة من الأبعاد.

حددت الدراسة مستويات تطبيق حوكمة المعلومات لجامعات الشرق الجزائري في 24 فقرة موزعة على 04 أبعاد.

أولا: الفرضية الرئيسية الثانية:"مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري متوسط"

تنبثق عن الفرضية الرئيسية أربع (04) فروض فرعية مرتبطة بأبعاد حوكمة المعلومات.

1.2.6مبدأ المسؤولية.

مبدأ المسؤولية أحد المبادئ الجوهرية التي تقوم عليها حوكمة المعلومات، يركز عل توضيح الأدوار والمسؤوليات بين الإدارة العليا والمصالح المشتركة بما يسهم في الحد من الممارسات العشوائية ودعم إتخاذ القرارات على أسس واضحة.

أ.إختبار الفرضية الفرعية الأولى:

"مستوى تطبيق المسؤولية متوسط في المكتبات المركزية لجامعات الشرق الجزائري"

ب.عرض وتحليل الفقرات المتعلقة بمبدأ المسؤولية.

تم تحليل آراء المبحوثين بإستخدام كل من المتوسط الحسابي والإنحراف المعياري، وإختبار T، الجدول أدناه يوضح ذلك.

جدول رقم (15): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجال الأول "المسؤولية"

المسؤولـــــية		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة.	التكرار	15	46	12	24	13	2.76	1.270	-1.952	0.054	متوسطة	1
	الوزن النسبي	13.6	41.8	10.9	21.8	11.8						
تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات فيالمكتبة.	التكرار	24	41	10	27	8	2.58	1.273	-3.444	0.001	منخفضة	4
	الوزن النسبي	21.8	37.3	9.1	24.5	7.3						
تم تحديد المسؤوليات لحفظ وحذف المعلومات.	التكرار	25	44	8	26	7	2.51	1.254	-4.105	0.000	منخفضة	5
	الوزن النسبي	22.7	40	7.3	23.6	6.4						
هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين.	التكرار	14	47	11	32	6	2.72	1.174	-2.517	0.013	متوسطة	2
	الوزن النسبي	12.7	42.7	10	29.1	5.5						
يتم تنظيم دورات تدريبية متنوعة لضمان أن جميع العاملين يفهمون ويؤدون مسؤولياتهم بفعالية ضمن إطار حوكمة المعلومات، مما يعزز من الأمان والإمتثال داخل المكتبات الجامعية.	التكرار	26	44	7	25	8	2.50	1.276	-4.109	0.000	منخفضة	6
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان إلتزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والإمتثال للمعايير والسياسات.	التكرار	14	48	16	26	6	2.65	1.137	-3.187	0.002	متوسطة	3
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
جميع فقرات المجال معا							2.62	0.52	-7.594	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

تشير النتائج إلى أن المتوسط الحسابي العام لجميع فقرات المجالبلغ (2.62)، مع إنحراف معياري قدره (0.52)، وقيمة tتساوي -7.594 ووفقا لمقياس الدراسة يظهر أن الاتجاه العام لآراء المبحوثين حول هذا المجال كان بين متوسط ومنخفض، مع قيمة إحتمالية دالة إحصائيًا عند (Sig = 0.000)مما يدل على صحة الفرضية الفرعية

الأولى 1.1.2.5- مستوى تطبيق مبدأ المسؤولية متوسط في المكتبات المركزية لجامعات الشرق الجزائري عند مستوى دلالة احصائية 5 0.0 α.

تم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة.

تشير نتائج الفقرة " توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة" إلى أن معظم أخصائي المعلومات يدركون وجود سياسات موثقة تتعلق بالمسؤولية عن المعلومات، ما يعكس وعيًا تنظيميًا مقبولًا. يرجع الباحث ذلك إلى جهود إدارة المكتبات محل الدراسة في وضع إجراءات مكتوبة، لكنها ربما لا تكون كافية لتصل إلى جميع الموظفين بوضوح أو لتترجم إلى ممارسات فعالة.

2. هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين.

تعكس نتيجة الفقرة " هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين" فهمًا نسبيًا جيدًا لتوزيع المسؤوليات، وتشير إلى وجود نوع من التنظيم الإداري في إسناد المهام المتعلقة بالمعلومات. ومع ذلك فإن المتوسط الحسابي لا يزال في المستوى المتوسط، ويرجع الباحث السبب إلى إمكانية وجود لبس أو نقص في التواصل المؤسسي بشأن من يتحمل المسؤولية فعليًا.

3. تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان إلتزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والإمتثال للمعايير والسياسات.

تعكس نتيجة الفقرة " تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان التزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والإمتثال للمعايير والسياسات" والتي جاءت متوسطة؛ وعيًا نسبيا بأهمية المسؤولية الفردية، مما يدل على إدراك العاملين لدورهم في حماية المعلومات. غير أن النتيجة تشير كذلك إلى الحاجة إلى جهود أكبر لتعزيز هذه الثقافة، ربما عبر التحفيز أو التأطير التنظيمي.

4. تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات في المكتبة.

تشير نتائج الفقرة " تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات في المكتبة" منخفضة رغم وجود سياسات، فإن فهم تفاصيلها خاصة الأدوار والمسؤوليات لا يبدو واضحًا لدى غالبية المبحوثين. هذا يشير إلى قصور في توصيل محتوى السياسات أو ضعف في عملية التوعية والتكوين بشأنها.

5. تم تحديد المسؤوليات لحفظ وحذف المعلومات.

تعكس نتيجة الفقرة " تم تحديد المسؤوليات لحفظ وحذف المعلومات." ضعفًا واضحًا في آليات تحديد المسؤوليات المتعلقة بدورة حياة المعلوماتخاصة الحذف، ما قد يُعرّض المكتبات محل الدراسة لمخاطر تتعلق بالتراكم العشوائي أو تسريب المعلومات الشخصية المتعلقة بالمستفيدين. ويرجح الباحث قد يعود ذلك إلى غياب الإجراءات أو نقص التدريب.

6. يتم تنظيم دورات تدريبية متنوعة لضمان أن جميع العاملين يفهمون ويؤدون مسؤولياتهم بفعالية ضمن إطار حوكمة المعلومات، مما يعزز من الأمان والإمتثال داخل المكتبات الجامعية.

تدل النتيجة المنخفضة للفقرة " يتم تنظيم دورات تدريبية متنوعة لضمان أن جميع العاملين يفهمون ويؤدون مسؤولياتهم بفعالية ضمن إطار حوكمة المعلومات، مما يعزز من الأمان والامتثال داخل المكتبات الجامعية " أن التدريب المؤسسي في مجال حوكمة المعلومات ما يزال محدودًا، أو غير منتظم. مما يُضعف قدرة الموظفين على فهم وتنفيذ المسؤوليات المتعلقة بالمعلومات، هذه الفجوة تتطلب تدخلًا من الإدارات العليا لتعزيز القدرات المهنية.

مما سبق نخلص أن نتائج عبارات المجال الأول "المسؤولية" تشير إلى مستوى متوسط فيما يتعلق بالمسؤولية عن إدارة وحماية المعلومات داخل المكتبات الجامعية، فقد أظهرت النتائج أن السياسات والإجراءات الخاصة بالمسؤوليات موجودة ومُوثقة نسبيًا، كما أن هناك نوعًا من التفويض والتنظيم في تسيير الملفات والمعلومات، إلى جانب إدراك معتدل لأهمية المسؤولية الفردية.

غير أن ضعف المتوسطات في بعض الفقرات؛ خاصة تلك المتعلقة بتحديد المسؤوليات الخاصة بالحذف والحفظ، وتنظيم الدورات التدريبية – يُبين وجود نقص في التكوين والتوعية، وكذلك قصور في تفعيل السياسات المعتمدة على المستوى العملي، وهذا ما يدعو إلى مراجعة شاملة لآليات التكوين الداخلي، وتعزيز ثقافة المسؤولية، وتوضيح الأدوار بطرق عملية قابلة للتطبيق، بما يحقق إنسجامًا أكبر مع متطلبات حوكمة المعلومات والإمتثال لمعايير الأمن السيبراني.

2.2.6مبدأ الإمتثال.

تزداد أهمية مبدأ الامتثال في ظل التوسع في إستخدام الموارد الرقمية وقواعد البيانات في المكتبات الجامعية، ما يرافق ذلك من تحديات تتعلق بسرية المعلومات وسلامتها وإتاحتها. كما يسهم مبدأ الإلتزام في الحد من المخاطر القانونية والأمنية، وضمان الإستخدام الآمن والمسؤول للمعلومات.

أ. إختبار الفرضية الفرعية الثانية.

"مستوى تطبيق الامتثال متوسط في المكتبات المركزية لجامعات الشرق الجزائري"

ب.عرض وتحليلالفقرات المتعلقة بمبدأ الإمتثال.

تم استخدام إختبار t للعينة الواحدة والجدول رقم (16) يبين آراء أفراد عينة الدراسة في فقرات "مبدأالإمتثال".

جدول رقم (16): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجالالثاني "الامتثال"

الإمتثـــــــال		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية	التكرار	16	39	11	32	12	2.86	1.288	1.110-	0.269	متوسطة	1
	الوزن النسبي	14.5	35.5	10	29.1	10.9						
يتم تنفيذ إجراءات في الكشف عن أي مخالفات أو عدم تطابق، مع المعايير الداخلية والخارجية؛ مما يسمح باتخاذ الإجراءات التصحيحية اللازمة للحفاظ على مستوى عالٍ من الامتثال والجودة".	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	6
	الوزن النسبي	25	40	6.4	22.7	7.3						
تتبنى المكتبة استراتيجية لإدارة مخاطر عدم الامتثال	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	2
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الامتثال وتوضيح المعايير والممارسات المطلوبة	التكرار	24	37	12	29	8	2.64	1.283	2.972-	0.004	متوسطة	4
	الوزن النسبي	21.8	33.6	10.9	26.4	7.3						
الرقابة المستمرة للاداء	التكرار	14	43	12	29	12	2.84	1.260	1.362	0.176	متوسطة	3

والاجراءات خلال تنفيذ الانشطة اليومية لضمان الالتزام الفوري للموظفين بالسياسات لمنع المشكلات قبل ان تحدث	الوزن النسبي	12.7	39.1	10.9	26.4	10.9			-		
يتم اجراء مراجعات دورية لتقييم منتظم للوائح والاجراءات لضمان التزامها بالمعايير بمرور الوقت .	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	5
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
جميع فقرات المجال معا							2.71	0.73	4.019-	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

تشير النتائج إلى أن المتوسط الحسابي العام لجميع فقرات المجال بلغ (2.71)، وهو ما يعكس مستوى متوسطًا بشكل عام، مع قيمة احتمالية دالة إحصائيًا عند (Sig = 0.000)مما يدل على أن مستوى الإمتثال متوسطة عند مستوى دلالة احصائية α 0.0 5.

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية.

تشير نتيجة الفقرة " تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية " إلى مستوى جيد نسبيًا لدى المكتبات الجامعية محل الدراسة بأهمية إحترام الإطار التشريعي والتنظيمي المتعلق بحوكمة المعلومات والخصوصية. ويفهم من ذلك أن هناك إلتزامًا رسميًا نسبيًا، وإن لم يكن قويًا بالتشريعات، وهو ما يعكس جهودًا تنظيمية على مستوى هذه المكتبات.

2. تتبنى المكتبة إستراتيجية لإدارة مخاطر عدم الإمتثال.

تدل نتيجة الفقرة " تتبنى المكتبة إستراتيجية لإدارة مخاطر عدم الإمتثال " على إدراك واضح بأهمية وضع خطة أو إطار عمل يخص التعامل مع حالات عدم الإمتثال المحتملة. هذا التبني يشير إلى فهم نظري مقبول، ولكن قد يفتقر إلى التنفيذ العملي الصارم داخل المؤسسات.

3. الرقابة المستمرة للأداء والإجراءات خلال تنفيذ الأنشطة اليومية لضمان الإلتزام الفوري للموظفين بالسياسات لمنع المشكلات قبل أن تحدث.

تعكس نتيجة الفقرة " الرقابة المستمرة للأداء والإجراءات خلال تنفيذ الأنشطة اليومية لضمان الإلتزام الفوري للموظفين بالسياسات لمنع المشكلات قبل أن تحدث " وجود مستوى لا بأس به من المراقبة والمتابعة أثناء تنفيذ الأنشطة اليومية. وهذا يُظهر سعي المكتبات محل الدراسة للإلتزام العملي بالسياسات، لكن النتيجة المتوسطة تؤكد أن الرقابة ليست شاملة أو منتظمة بالشكل الكافي.

4. توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الامتثال وتوضيح المعايير والممارسات المطلوبة.

تشير نتيجة الفقرة " توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الإمتثال وتوضيح المعايير والممارسات المطلوبة " إلى وجود بعض الجهود التدريبية من قبل المكتبات الجامعية، لكنها محدودة. فالتدريب لا يزال غير كافٍ لترسيخ ثقافة الإمتثال الكامل داخل المكتبات الجامعية ويحتاج إلى مزيد من الدعم والمتابعة.

5. يتم إجراء مراجعات دورية لتقييم منتظم للوائح والإجراءات لضمان إلتزامها بالمعايير بمرور الوقت.

الفقرة " يتم اجراء مراجعات دورية لتقييم منتظم للوائح والاجراءات لضمان التزامها بالمعايير بمرور الوقت "تشير إلى نتيجة متوسطة، تُبرز أن عملية التقييم الدوري موجودة لكنها ربما لا تتم بإنتظام أو لا تشمل كل الجوانب المطلوبة لتضمن تحديث السياسات وتطابقها مع المستجدات التشريعية.

6. يتم تنفيذ إجراءات في الكشف عن أي مخالفات أو عدم تطابق، مع المعايير الداخلية والخارجية؛ مما يسمح بإتخاذ الإجراءات التصحيحية اللازمة للحفاظ على مستوى عالٍ من الإمتثال والجودة.

الفقرة" يتم تنفيذ إجراءات في الكشف عن أي مخالفات أو عدم تطابق، مع المعايير الداخلية والخارجية؛ مما يسمح بإتخاذ الإجراءات التصحيحية اللازمة للحفاظ على مستوى عالٍ من الإمتثال والجودة" أضعف فقرات المجال، تُشير إلى وجود قصور واضح في الإجراءات الخاصة بإكتشاف ومعالجة حالات عدم الإمتثال، وهذا يمثل نقطة ضعف خطيرة يجب معالجتها لتفادي المخاطر السيبرانية وتحقيق حوكمة معلومات فعالة.

ومما سبق نخلص إلى أن نتائج عبارات المجال الثاني " مبدأ الإمتثال"تشير إلى أن درجة الإمتثال داخل المكتبات الجامعية محل الدراسة متوسطة إجمالًا، مع وجود مستوى تنظيمي أساسي، لكنه غير مدعوم بإجراءات رقابية صارمة أو برامج تدريبية كافية. وعليه ينصح الباحث بتقوية جانب الرقابة والكشف، وزيادة برامج التوعية والتقييم الدوري، لضمان توافق أكبر مع مبادئ حوكمة المعلومات والأمن السيبراني.

3.2.6مبدأ الحفظ.

يكتسب مبدأ الحفظ أهمية خاصة نظرًا لما تمتلكه المكتبات من موارد معلوماتية متنوعة، ورقية ورقمية ويقصد به وضع السياسات والإجراءات التي تضمن الإحتفاظ بالمعلومات، منذ إنشائها أو اقتنائها وحتى إتلافها أو حفظها الدائم، بما يضمن إستمرارية الوصول إليها وحمايتها من الضياع أو التلف أو الاستخدام غير المشروع.

أ. إختبار الفرضية الفرعية الثالثة:

"مستوى تطبيق الحفظ متوسط في المكتبات المركزية لجامعات الشرق الجزائري"

ب. عرض وتحليل الفقرات المتعلقة بمبدأ الحفظ.

تم إستخدام إختبار(**t**) للعينة الواحدة لتحليل آراء أفراد عينة الدراسة حول فقرات **مبدأ الحفظ**، كما هو موضح في الجدول أدناه، الذي يبيّن المتوسطات الحسابية، والإنحرافات المعيارية، وقيم الإختبار الإحصائي، ومستويات الدلالة لفقرات المجال الثالث.

الجدول رقم (17) : المتوسط الحسابي وقيمة الاحتمال (Sig.) لجميع فقرات المجالالثالث "الحفظ"

الحفـــــظ		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (Sig.)	درجة التبني	الترتيب
تلتزم المكتبة بمبدأ الحفاظ على المعلومات للفترة الزمنية اللازمة وفقًا للمتطلبات القانونية والتنظيمية	التكرار	27	42	7	26	8	2.51	1.290	3.990-	0.000	منخفضة	6
	الوزن النسبي	24.5	38.2	6.4	23.6	7.3						
تستخدم المكتبة (الوسائل؛ مواد؛ برمجيات)للحفظ الآمن؛وأرشفة المعلومات	التكرار	13	48	16	27	6	2.68	1.133	2.946-	0.004	متوسطة	2
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
تتبع المكتبة سياسات وإجراءات لحفظ المعلومات والحفاظ على سلامتها وإستمراريتها وبشكل صحيح ومنظم	التكرار	26	43	7	26	8	2.52	1.283	3.938-	0.000	منخفضة	5
	الوزن النسبي	23.6	39.1	6.4	23.6	7.3						
تتم مراجعة وتحديث سياسات حفظ المعلومات بإنتظام وفقا للمتطلبات القانونية والتنظيمية والتشغيلية.	التكرار	14	48	16	26	6	2.65	1.137	3.187-	0.002	متوسطة	3
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
تستخدم المكتبة تقنيات	التكرار	25	43	8	26	8	2.54	1.276	3.812	0.000	منخفضة	4

الأرشفة الملائمة للمحافظة على المعلومات بشكل دائم	الوزن النسبي	22.7	39.1	7.3	23.6	7.3			-		
تطبق المكتبة إجراءات النسخ الاحتياطي الدوري واختبار الاسترجاع لضمان استمرارية المعلومات وإتاحتها عند الحاجة.	التكرار	14	47	11	32	6	2.72	1.174	2.517-	0.002	متوسطة	1
	الوزن النسبي	12.7	42.7	10	29.1	5.5						
جميع فقرات المجال معا							2.60	0.66	6.217-	0.000	منخفضة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

تشير النتائج العامة إلى أن المتوسط الحسابي الكلي لجميع فقرات مجال الحفظ بلغ (2.60)، بإنحراف معياري قدره (0.66)، مع قيمة دلالة إحصائية معنوية عند مستوى(Sig = 0.000) ، وهو ما يدل على أن مستوى تطبيق مبدأ الحفظ في المكتبات الجامعية محل الدراسة جاء بمستوى منخفض عند مستوى دلالة إحصائية (0.05) .
وعليه فإن نتائج هذا المجال لا تدعم الوصول إلى مستوى متوسط في تطبيق مبدأ الحفظ، بل تعكس وجود قصور واضح في هذا البعد من أبعاد حوكمة المعلومات.

ولتفسير هذه النتائج بشكل أدق، تم ترتيب فقرات هذا المجال ترتيبًا تنازليًا حسب المتوسط الحسابي لكل فقرة، وتحليلها على النحو الآتي:

1. إستخدام المكتبة للوسائل والمواد والبرمجيات الخاصة بالحفظ الآمن وأرشفة المعلومات

أظهرت الفقرة المتعلقة بإستخدام المكتبة للوسائل والمواد والبرمجيات الخاصة بالحفظ الآمن وأرشفة المعلومات متوسطًا حسابيًا قدره (2.68)، ما يشير إلى وجود اعتماد نسبي على بعض الأدوات التقنية في مجال الحفظ، غير أن هذا الاعتماد لا يزال محدودًا ولا يعكس تطبيقًا منهجيًا متكاملًا.

2. مراجعة وتحديث سياسات حفظ المعلومات بانتظام وفق المتطلبات القانونية والتنظيمية والتشغيلية.

سجلت الفقرة الخاصة بمراجعة وتحديث سياسات حفظ المعلومات بانتظام وفق المتطلبات القانونية والتنظيمية والتشغيلية متوسطًا حسابيًا بلغ (2.65)، وهو ما يدل على وجود بعض الممارسات التنظيمية في هذا الجانب، لكنها لا تزال دون المستوى المطلوب من حيث الإنتظام والفعالية.

3.إلتزام المكتبة بالحفاظ على المعلومات للفترة الزمنية اللازمة وفق المتطلبات القانونية والتنظيمية.

في المقابل، جاءت عدة فقرات بمستوى منخفض، من بينها الفقرة المتعلقة بالتزام المكتبة بالحفاظ على المعلومات للفترة الزمنية اللازمة وفق المتطلبات القانونية والتنظيمية، والتي سجلت متوسطًا حسابيًا قدره (2.51)، مما يعكس ضعف الالتزام العملي بإدارة مدد الاحتفاظ بالمعلومات.

4.إتباع المكتبة لسياسات وإجراءات واضحة لحفظ المعلومات والحفاظ على سلامتها وإستمراريتها.

أظهرت الفقرة المتعلقة بإتباع المكتبة لسياسات وإجراءات واضحة لحفظ المعلومات والحفاظ على سلامتها وإستمراريتها متوسطًا حسابيًا منخفضًا بلغ (2.52)، وهو ما يشير إلى غياب أو ضعف تفعيل السياسات المعتمدة، رغم وجودها الشكلي في بعض الحالات.

5.استخدام تقنيات الأرشفة الملائمة للمحافظة على المعلومات بشكل دائم.

سجلت الفقرة الخاصة باستخدام تقنيات الأرشفة الملائمة للمحافظة على المعلومات بشكل دائم متوسطًا حسابيًا قدره (2.54)، ما يعكس محدودية توظيف تقنيات الأرشفة الحديثة، وعدم كفاية البنية التقنية الداعمة لحفظ المعلومات على المدى الطويل.

في الأخير، تُظهر نتائج مجال الحفظ أن هذا البعد يُعد من أضعف أبعاد حوكمة المعلومات في المكتبات الجامعية محل الدراسة، حيث يتسم بضعف في الإلتزام بالمتطلبات القانونية والتنظيمية، ومحدودية في إستخدام التقنيات الملائمة إلىجانب قصور في تفعيل السياسات والإجراءات المرتبطة بحفظ المعلومات وإستمراريتها. ويشير ذلك إلى وجود فجوة واضحة بين الإطار النظري لمبدأ الحفظ والتطبيق العملي له داخل هذه المكتبات.

4.2.6 مبدأ الإستبعاد.

يشير مبدأ الإستبعاد إلى تحديد المعلومات والبيانات التي يجب حصر الوصول إليها أو منع تداولها أو مشاركتها خارج نطاق محدد، وذلك حفاظًا على سرية المعلومات وحمايتها من الإستخدام غير المصرح به. يهدف هذا المبدأ إلى الحد من المخاطر المرتبطة بتسريب المعلومات، وضمان أن الوصول إلى الموارد المعلوماتية يتم وفق سياسات واضحة.

أ. الفرضية الفرعية الرابعة:

"مستوى تطبيق الاستبعاد متوسط في المكتبات المركزية لجامعات الشرق الجزائري "

ب. عرض وتحليل الفقرات المتعلقة بمبدأ الاستبعاد.

تم استخدام إختبار t للعينة الواحدة والنتائج المبينة في جدول رقم (18) يبينآراء أفراد عينة الدراسة في فقرات"مبدأالإستبعاد".

جدول رقم (18) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجالالرابع "الاستبعاد"

الإستبعـــــاد		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
يتم إستبعاد المعلومات المتعلقة بمصادر المعلومات والمعطيات الشخصية بشكل منتظم وفقا للسياسات والمتطلبات القانونية	التكرار	13	42	11	33	11	2.88	1.247	0.994-	0.322	متوسطة	1
	الوزن النسبي	11.8	38.2	10	30	10						
يتم الإستبعاد تلقائيا للمعلومات المخزنة إكترونيا بشكل نهائي من وسائل الإتاحة.	التكرار	23	39	11	29	8	2.64	1.276	2.989-	0.003	متوسطة	4
	الوزن النسبي	20.9	35.5	10	26.4	7.3						
تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات.	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	2
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
توفر المكتبة برامج للتوعية والتدريب المستمر بشأن ترتيبات المصير النهائي للمعلومات	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	5
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
توثق المكتبة جميع الإجراءات المتعلقة بترتيبات المصير النهائي للمعلومات.	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	6
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
يتم تقييم مدى إلتزام المكتبة بسياسات الاستبعاد وتحسين فعالية الاجراءات المتبعة.	التكرار	14	48	16	26	6	2.65	1.137	3.187-	0.002	متوسطة	3
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
جميع فقرات المجال معا							2.68	0.61	5.299-	0.000	**متوسطة**	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يظهر الجدول أعلاه،أن المتوسط الحسابي لجميع فقرات "الإستبعاد " تساوي (2.68)، وهو ما يعكس مستوى متوسطة، مع قيمة إحتمالية دالة إحصائيًا عند (Sig = 0.000) مما يدل على أن مستوى الإستبعاد متوسطة عند مستوى دلالة إحصائية α 0.0 5.

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي :

1. يتم إستبعاد المعلومات المتعلقة بمصادر المعلومات والمعطيات الشخصية بشكل منتظم وفقا للسياسات والمتطلبات القانونية.

تشير نتيجة الفقرة " يتم استبعاد المعلومات المتعلقة بمصادر المعلومات والمعطيات الشخصية بشكل منتظم وفقا للسياسات والمتطلبات القانونية " إلى وجود إلتزام نسبي بعمليات إستبعاد المعلومات الحساسة وفقًا للسياسات القانونية. رغم كون الدرجة "متوسطة"، فإنها تعكس وعيًا بأهمية حماية الخصوصية، إلا أن هذا الوعي لم يصل بعد إلى مستوى مرتفع من التطبيق العملي أو المؤسسي.

2. تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات.

تدل نتيجة الفقرة " تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات." على أن بعض المكتبات الجامعية تعتمد تصنيفًا للمعلومات يُحدد ما يجب الإحتفاظ به وما يجب التخلص منه. وهذا مؤشر جيد على تطبيق مبادئ الحوكمة، لكنه بحاجة إلى تحسين في الدقة والاتساق.

3. يتم تقييم مدى إلتزام المكتبة بسياسات الإستبعاد وتحسين فعالية الإجراءات المتبعة.

يتم تقييم مدى إلتزام المكتبة بسياسات الإستبعاد وتحسين فعالية الإجراءات المتبعة يدل متوسط الفقرة " يتم تقييم مدى إلتزام المكتبة بسياسات الإستبعاد وتحسين فعالية الإجراءات المتبعة." على وجود بعض الجهود لمراقبة فعالية عمليات الإستبعاد، ولكن هذه الممارسات ليست منهجية أو مؤسسية بشكل كافٍ، مما يؤثر على جودة التقييم وإستمراريته.

4. يتم الإستبعاد تلقائيا للمعلومات المخزنة إلكترونيا بشكل نهائي من وسائل الإتاحة.

تعكس نتيجة الفقرة " يتم الإستبعاد تلقائيا للمعلومات المخزنة إلكترونيا بشكل نهائي من وسائل الإتاحة "بروز جزئيً للحلول الرقمية المؤقتة في عمليات الحذف، ولكن ذلك لا يتم بشكل دائم أو متكامل. وقد يشير أيضًا إلى ضعف في أنظمة إدارة دورة حياة المعلومات أو في عدم تكامل الأدوات التقنية المستخدمة.

5. توفر المكتبة برامج للتوعية والتدريب المستمر بشأن ترتيبات المصير النهائي للمعلومات.

تشير نتيجة الفقرة " توفر المكتبة برامج للتوعية والتدريب المستمر بشأن ترتيبات المصير النهائي للمعلومات " إلى وجود جهود محدودة في تدريب العاملين على كيفية التعامل مع المعلومات التي بلغت نهاية دورتها. هذا النقص قد يُؤثر سلبًا على فعالية عمليات الإستبعاد ويزيد من إحتمالية الإحتفاظ غير المبرر بالمعلومات.

6. توثق المكتبة جميع الإجراءات المتعلقة بترتيبات المصير النهائي للمعلومات.

أظهرت معطيات الجدول أن فقرة" توثق المكتبة جميع الإجراءات المتعلقة بترتيبات المصير النهائي للمعلومات " أدنى فقرات المجال تقييمًا، مما يكشف عن قصور واضح في توثيق السياسات والإجراءات الخاصة بعمليات الإستبعاد، وهذا يمثل خطرًا كبيرًا في مجال الحوكمة، حيث يعيق المراجعة والمساءلة ويزيد من إحتمالات سوء التعامل مع المعلومات.

مما سبق نخلص إلى القول أن نتائج عبارات المجالالرابع (الإستبعاد) تشير إلى أن درجة الإستبعاد داخل المكتبات الجامعية محل الدراسة متوسطة بوجه عام، مع وجود خلل ملحوظ في توثيق الاجراءات وضعف في البرامج التوعوية والتقنية.

ثانيا:إختبار الفرضية الثانية الرئيسية:

"مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري متوسط".

ثالثا:تحليل مستوى تطبيق حوكمة المعلومات بالمكتبات الجامعية.

تم استخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (19) والذي يبين اراء افراد عينة الدراسة لجميع مجالات المحور الثاني (مستوى حوكمة المعلومات بالمكتبات الجامعية) .

جدول رقم (19) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المحور الثاني "مستوى تطبيق مبادئ حوكمة المعلومات"

الأبعاد	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	الترتيب
المســـؤولية	2.62	0.52	-7.594	0.000	3

الامتثـــــال	2.71	0.73	-4.020	0.000	1
الحفـــــظ	2.60	0.66	-6.381	0.000	4
الاستبعـــــاد	2.68	0.61	-5.373	0.000	2
مستوى تطبيق مبادئ حوكمة المعلومات	2.65	0.50	-7.064	0.000	متوسطة

الارتباط دال احصائيا عند مستوى $\alpha \leq 0.05$.

يتبين أن المتوسط الحسابي لجميع مجالات المحور الأول تساوي (2.65)، وقيمةt المحسوبة تساوي -7.064 أما القيمة الاحتمالية تساوي 0.000 وهي اقل من 0.05 مما يدل على أن مستوى حوكمة المعلومات متوسطة عند مستوى دلالة احصائية α 0.0 5.

ويرى الباحث أن مستوى حوكمة المعلومات يتراوح بين المتوسط والمنخفض. فقد جاء بعد "الامتثال"في المرتبة الأولى بمتوسط حسابي نسبي بلغ (2.71)، ما يعكس وجود وعي نسبي لدى المكتبات الجامعية بضرورة الالتزام بالتشريعات والمعايير المرتبطة بحوكمة المعلومات، وإن كانت بعض فقراته لا تزال تسجل مستويات تبنٍ منخفضة، مثل ضعف تنفيذ إجراءات الكشف عن المخالفات أو المراجعة الدورية للامتثال. يلي ذلك بعد "الاستبعاد"في المرتبة الثانية (2.68)، مما يدل على وجود سياسات مبدئية لإدارة المصير النهائي للمعلومات، إلا أنها تفتقر في بعض الجوانب إلى الموثوقية والانتظام، خاصة في ما يتعلق بالتوثيق والتدريب المستمر.

أما بعد "المسؤولية"فقد جاء في المرتبة الثالثة بمتوسط حسابي نسبي (2.62)، وهو ما يشير إلى وجود توجه عام نحو تحديد المسؤوليات وتوزيعها، مع ضعف واضح في التدريب وتعزيز ثقافة المسؤولية الفردية. في حين احتل بعد "الحفظ"المرتبة الأخيرة (2.60)، ما يُبرز قصورًا في الالتزام بمدة الاحتفاظ القانونية أو استخدام أدوات وتقنيات أرشفة حديثة، وهو مؤشر مقلق نظرًا لأهمية هذا البعد في دورة حياة المعلومات.

بناءً على هذه النتائج، يُمكن القول أن مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات الجامعية محل الدراسة هو متوسط بصفة عامة، ويُظهر تباينًا في تطبيق الأبعاد الأربعة، مما يتطلب مجهودًا مؤسساتيًا ممنهجًا لتعزيز ثقافة الحوكمة، خاصة في مجالات الحفظ وتوزيع المسؤوليات، مع التركيز على التحسين المستمر ومراجعة السياسات والإجراءات بإنتظام.

3.6 مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية.

تتعرض الأنظمة والبيانات الرقمية إل العديد من التهديدات والأضرار نتيجة هجمات إلكترونية أو أخطاء بشرية أو خلل تقني، والتي قد تتسبب في فقدان السرية والأمان. وعيه فإن تدارك هذه المخاطر ضرورة لضمان حماية البيانات وتحقيق الإستمرارية.

أولا: الفرضية الرئيسية الثالثة:" مستوى مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي".

تنبثق عن الفرضية الرئيسية الثالثة أربع (04) فرضيات فرعية، بهدف الوقوف على مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة، إعتمد الباحث على 24 فقرة موزعة على 04 أبعاد وهي: السرية والسلامة ، التوافر والمخاطر العامة.

1.3.6 مبدأ السرية

تكتسب السرية في المكتبات الجامعية أهمية خاصة نظرًا لما تحتويه من بيانات أكاديمية وبحثية، إضافة إلى المعلومات الشخصية الخاصة بالمستفيدين والموظفين. ويسهم الإلتزام بمبدأ السرية في تعزيز الثقة بين المكتبة ومستفيديها، والحد من مخاطر الأمن السيبراني، كما يرتبط مبدأ السرية إرتباطًا وثيقًا ببقية مبادئ حوكمة المعلومات، مثل المسؤولية والامتثال والإستبعاد. يتطلب تطبيقه وضع سياسات واضحة للتحكم في الوصول إلى المعلومات.

أ. إختبار الفرضية الفرعية الأولى:

"مستوى السريةعالي في المكتبات المركزية لجامعات الشرق الجزائري "

ب.عرض وتحليل الفقرات المتعلقة بمبدأ السرية.

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (20) يظهرآراء أفراد عينة الدراسة لجميع فقرات المجال الأول "السرية".

جدول رقم (20) : المتوسط الحسابي وقيمة الاحتمال (Sig.) لجميع فقرات المجالالأول "السرية"

السرية	غير موافق	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار	القيمة الاحتمالية	درجة التبني	الترتيب

		بشدة						T	(.Sig)		
هجمات التنصت (إعتراض شبكة الاتصالات او التقاط البيانات اثناء نقلها داخل وخارج المكتبة).	التكرار	27	36	11	28	8	2.58	1.302	3.369-	0.001	منخفضة	6
	الوزن النسبي	24.5	32.7	10	25.5	7.3						
هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام او المنقولة عبر الشبكة).	التكرار	24	41	7	30	8	2.61	1.293	3.171-	0.002	متوسطة	5
	الوزن النسبي	21.8	37.3	6.4	27.3	7.3						
الوصول غير المصرح به لنظام المكتبة من قبل اطراف خارجية مثل المهاجمين	التكرار	25	44	8	26	7	2.51	1.254	4.105-	0.000	منخفضة	7
	الوزن النسبي	22.7	40	7.3	23.6	6.4						
الوصول غير المصرح به لنظام المكتبة من قبل اطراف داخلية مثل المكتبيين(الموظفين)	التكرار	14	47	11	32	6	2.72	1.174	2.517-	0.013	متوسطة	3
	الوزن النسبي	12.7	42.7	10	29.1	5.5						
الافعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة).	التكرار	14	47	12	24	13	2.77	1.261	1.890-	0.061	متوسطة	2
	الوزن النسبي	12.7	42.7	10.9	21.8	11.8						
الافعال المتعمدة المتعلقة بالابتزاز(الابتزاز بالكشف عن المعلومات	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	1
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
هجمات الاصطياد الالكتروني؛ انتحال هوية اشخاص او منظمة يثق بهم الضحية باستخدام وسائل تقنية.	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	4
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
هجمات الهندسة الاجتماعية (القدرة على التمثيل واقناع الضحية بالإفصاح عن المعلومات السرية).	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	8
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
جميع فقرات المجال معا							2.64	0.56	6.612-	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

يوضح الجدول أعلاه،أن المتوسط الحسابي لجميع فقرات المجال الأول (السرية) تساوي (2.64)، وقيمة t المحسوبة تساوي (-6.612) اما القيمة الاحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على ان مستوى السرية متوسطة عند مستوى دلالة إحصائية α 0.0 5.

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات المركزية عينة الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. الأفعال المتعمدة المتعلقة بالإبتزاز (الابتزاز بالكشف عن المعلومات).

تشير نتائج الفقرة " الأفعال المتعمدة المتعلقة بالإبتزاز(الابتزاز بالكشف عن المعلومات)"أنعددمعتبر من المبحوثين يرون أن الإبتزاز المرتبط بالمعلومات الشخصية والتي تعتبر حساسة يمثل تهديدا قائما في بيئة المكتبات الجامعية ، لا سيما في ظل ضعف أو محدودية إجراءات حماية البيانات.

ويعزز هذا التصور المتوسط الحسابي (2.85) الذي يقع ضمن مستوى المتوسط مما يعكس وعيا جزئيا أو منفاوتا بوجود هذا النوع من المخاطر.غير أن القيمة الإحتمالية (sig :0.203) التي تفوق مستوى الدلالة الإحصائية المعتمد(0.05) تشير إلى عدم وجود إتفاق قوي بين آراء أفراد العينة بشأن هذا التهديد. ينسب الباحث هذا التباين إلى درجة إنكشاف المكتبات الجامعية لمثل هذه الحالات أو غياب سياسات واضحة للإبلاغ والتعامل مع حوادث الإبتزاز المعلوماتي.

2. الأفعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة).

تدل نتائج الفقرة " الأفعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة)." على وجود تصور عام لدى المبحوثين بأن المكتبات الجامعية مهددة بسرقة معدات أو معلومات. ويستدل على ذلك من المتوسط الحسابي الذي جاء في مستوى متوسط مما يشير إلى إدراك نسبي لوجود هذه المخاطر.

غير أن القيمة الإحتمالية (Sig = 0.061) التي تفوق مستوى الدلالة المعتمد (0.005) تظهر أن الفروق في الإجابات ليست ذات دلالة احصائية ، مما يعكي تباينا في وجهات نظر المبحوثين حول شدة هذه التهديدات .

ويرجع الباحث هذا التباين إلى إختلاف الخبرات الشخصية، وتفاوت فعلي في تطبيق أنظمة الحماية الفيزيائية والرقمية بين مكتبة وأخرى، الأمر الذي يستدعي تعزيز سياسات الأمان المادي والرقمي بشكل موحد في المكتبات الجامعية.

3. الوصول غير المصرح به لنظام المكتبة من قبل أطراف داخلية مثل المكتبيين(الموظفين)

تشير نتائج الفقرة " الوصول غير المصرح به لنظام المكتبة من قبل أطراف داخلية مثل المكتبيين(الموظفين)"إلى وجود إدراك نسبي واضح بأن التهديدات قد تنشأ من داخل المكتبة نفسها، ويبرز ذلك أهمية تطبيق مبدأ"الحد الادنى من الإمتيازات " في صلاحيات الدخول، والمراقبة المستمرة للأنشطة الداخلية.

ويرى الباحث عدم دلالة الفقرة إحصائيا (sig> 0.05) يوحي بعدم وجود إجماع قوي والذي نرجعه الى اختلاف التجارب أو الخبرات بين أفراد العينة وإلى ضعف الوعي لمفهوم الإبتزاز المعلوماتي مع قلة الحوادث الفعلية التي يمكن أن تترك أأثر مشتركا.

4. هجمات الإصطياد الإلكتروني؛ إنتحال هوية أشخاص أو منظمة يثق بهم الضحية بإستخدام وسائل تقنية.

نتائج الفقرة " هجمات الإصطياد الالكتروني؛ إنتحال هوية أشخاص أو منظمة يثق بهم الضحية بإستخدام وسائل تقنية."إلى أن هذا النوع من الهجمات يعد تهديدا فعليا ومعترفا به من قبل أفراد العينة، كما يدل عليه المتوسط الحسابي (2.62) الذي يعكس درجة تبني متوسطة؛ ويعزز هذا التوجه القيمة الاحتمالية (sig :0.002) التي تقل عن مستوى الدلالة (0.05) ، ما يعني وجود إتفاق دال إحصائيا بين المبوحثين حول خطورة هذه الهجمات

5. هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام او المنقولة عبر الشبكة).

تعكس نتائج الفقرة " هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام أو المنقولة عبر الشبكة)."إلى أن كلمات المرور تمثل تهديد حقيقي وفقا لآراء المبحوثين ، حيث بلغ المتوسط الحسابي (2.61) مما يعكس درجة تبني متوسطة؛ وتعد النتيجة دالة احصائيا (Sig = 0.002 < 0.05)، ما يدل على وجود اتفاق معنوي بين افراد العينة حول ضعف كلمات المرور كأحد أبرز منافذ الهجمات السيبرانية.

يرى الباحث أن المبحوثين على وعي بالمخاطر المرتبطة بهذا النوع من الهجمات داخل المكتبات الجامعية وهو ناتج عن خبرات سابقة أو حوادث تعرضت فيها أنظمة المكتبات إلى الإختراق أو التهديد نتيجة كلمات مرور ضعيفة أو غير محمية .

كما يلاحظ الباحثإ ان درجة التبني المتوسطة تشير إلى وجود تفاوت في مستوى الإجراءات الأمنية المطبقة فعليا بين مختلف المكتبات وهو ما يظهر ضرورة الإستثمار في أدوات التحقق القوية وتحديث سياسات أمن المعلومات المتعلقة بكلمات المرور بشكل دوري.

6. هجمات التنصت (إعتراض شبكة الإتصالات أو إلتقاط البيانات أثناء نقلها داخل وخارج المكتبة).

تبرز نتائج الفقرة "هجمات التنصت (إعتراض شبكة الاتصالات أو التقاط البيانات أثناء نقلها داخل وخارج المكتبة)."إلى وجود إدراك محدود لدى أفراد العينة بخطورة هجمات التصنت،الذي يعد من أخطر التهديدات التي تمس مبدأ السرية في مثلث أمن المعلومات. ويرى الباحث أن البيئات الأكاديمية التي تعتمد على نقل المعلومات عبر شبكات محلية أو الأنترنت تصبح البيانات عرضة لإعتراضها من جهات غير مخولة، مما يهدد الخصوصية خاصة عندما تتعلق المعلومات مستفيدين أو مستخدمين أو بمحتوى علمي حساس.

رغم دلالة النتائج إحصائيا، إلا أن درجة التبني المنخفضة تعكس تباين مستوى الفهم التقني لهذه الهجمات لذا يوصي الباحث بأن تعتمد المكتبات الجامعية محل الدراسة سياسات أمن المعلومات تراعي الحماية أثناء النقلمن خلال بروتوكولات وتقنين إستخدام الشبكات مع تضمين موضوعات متقدمة في البرامج التدريبية للأمن السيبراني داخل المكتبات.

7. الوصول غير المصرح به لنظام المكتبة من قبل أطراف خارجية مثل المهاجمين.

تشير نتائج الفقرة "الوصول غير المصرح به لنظام المكتبة من قبل أطراف خارجية مثل المهاجمين" إلى أن هناك إدراكًا مشتركًا بين أفراد العينة لوجود هذا النوع من التهديدات، وهو ما تؤكده الدلالة الإحصائية (Sig = 0.000)، التي تعكس اتفاقًا معنويًا بين المبحوثين. ومع ذلك، فإن المتوسط الحسابي المنخفض (2.51) يدل على أن هذا التهديد لا يُقابَل بدرجة تبنٍ عالية، مما يعني أن المبحوثين لا يولون هذا الخطر أهمية كافية أو لا يشعرون بضرورة التصدي له بشكل فعّال.

يرى الباحث أن هذا التناقض قد يُعزى إلى ثقة مفرطة في قدرة الأنظمة التقنية على الحماية أو إلى قلة الحوادث الفعلية المبلغ عنها؛ أو حتى غياب سياسات مؤسسية واضحة للتعامل مع مثل هذه الهجمات؛ وعليه فإن هذه النتيجة تعكس فجوة بين وعي نظري بوجود التهديد وضعف في التفاعل العملي معه، مما يستدعي تعزيز التدريبات والتوعية الأمنية، إلى جانب تطوير بنية تحتية تقنية أكثر صلابة لرصد ومنع محاولات الوصول غير المشروع.

8.عدم إدراك حجم التهديد الذي تمثله هذه الهجمات

أن المبحوثين لا يدركون بدرجة كافية حجم التهديد الذي تمثله هذه الهجمات، حيث جاء المتوسط الحسابي منخفضًا (2.50)، ما يعكس تبنّيًا ضعيفًا لها كمصدر تهديد فعلي. ورغم ذلك، فإن الدلالة الإحصائية (Sig = 0.000) تشير إلى وجود تصور عام، ولو محدود، لدى أفراد العينة بشأن خطورة هذه الهجمات. ويعزو الباحث هذا التباين إلى ضعف الثقافة الأمنية الرقمية داخل بيئة العمل المكتبية، وهو ما يُفضي إلى اعتقاد خاطئ بأن تهديدات الأمن السيبراني تقتصر فقط على الوسائل التقنية كالفيروسات أو الاختراقات المباشرة، دون الانتباه إلى خطورة العنصر البشري كمدخل أساسي للاختراق من خلال الخداع النفسي. هذا يبرز الحاجة إلى إدراج الهندسة الاجتماعية ضمن برامج التوعية والتدريب الأمني للمكتبيين.

وتُعتبر هذه الهجمات من أخطر التهديدات الناعمة، إذ لا تعتمد على أدوات تقنية متقدمة، بل على استغلال الثقة والعواطف والسلوك البشري، وهي غالبًا ما تكون بوابة الدخول الأولى للهجمات السيبرانية الأكثر تعقيدًا مثل سرقة الهوية أو تثبيت برمجيات خبيثة.

2.3.6 السلامة.

يكتسب مبدأ السلامة أهمية كبيرة نظرًا لإعتمادها على قواعد البيانات الرقمية، والمستودعات المؤسسية والأنظمة الآلية لإدارة المكتبات ويسهم تطبيق مبدأ السلامة في الحد من مخاطر الأمن السيبيراني.

أ.إختبار الفرضية الفرعية الثانية.

"مستوى السلامة عالي في المكتبات المركزية لجامعات الشرق الجزائري "

ب. عرض وتحليل الفقرات المتعلقة بمبدأ السلامة.

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (21) والذي يبين آراء أفراد عينة الدراسة لجميع فقرات المجال (السلامة).

جدول رقم (21): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجالالثاني "السلامة"

السلامة		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
الادخال الغير متعمد للبيانات الخاطئة من قبل الموظفين	التكرار	14	48	16	26	6	2.80	1.148	1.828-	0.070	متوسطة	2
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
اتلاف البيانات غير متعمد من قبل الموظفين	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	6
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
اتلاف البيانات المتعمد من قبل الموظفين	التكرار	14	48	16	26	6	2.65	1.137	3.187-	0.002	متوسطة	4
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
الادخال المتعمد للبيانات الخاطئة من قبل الموظفين .	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	1
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
اخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين اثناء كتابة البرامج.	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	5
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
التقادم التكنولوجي مثل الاجهزة والانظمة المتقادمة.	التكرار	14	47	12	24	13	2.77	1.261	1.890-	0.061	متوسطة	3
	الوزن النسبي	12.7	42.7	10.9	21.8	11.8						
جميع فقرات المجال معا							2.69	0.58	5.442-	0.000	**متوسطة**	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يتبين أن المتوسط الحسابي لجميع فقرات المجال الثاني (السلامة) تساوي (2.69)، وقيمة t المحسوبة تساوي (-5.442) اما القيمة الاحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على أن مستوى السلامة متوسطة عند مستوى دلالة إحصائية α 0.0 5.

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. الإدخال المتعمد للبيانات الخاطئة من قبل الموظفين .

تشير نتائج هذه الفقرة" الادخال المتعمد للبيانات الخاطئة من قبل الموظفين " إلى أن عددًا معتبرًا من المبحوثين يعتقدون بإمكانية حدوث إدخالات متعمدة لبيانات خاطئة من قبل الموظفين، وهو ما قد يعكس سلوكيات

مقصودة ناتجة عن سوء نية أو ضعف في الالتزام المهني داخل المكتبة الجامعية. ويؤكد هذا التصور المتوسط الحسابي البالغ (2.85)، والذي يقع ضمن مستوى التبني المتوسط، مما يعكس وجود درجة من الوعي بهذه الإشكالية، وإن كانت غير مرتفعة.

غير أن القيمة الاحتمالية(Sig = 0.203) ، التي تفوق مستوى الدلالة الإحصائية المعتمد (0.05)، تشير إلى أن هذا التصور لا يحظى بإجماع واضح بين أفراد العينة، مما يعكس تباينًا في الآراء قد يكون ناتجًا عن اختلاف في الخبرة أو في طبيعة المؤسسات التي ينتمي إليها المبحوثون.

يرجع الباحث هذا التباين إلى احتمالية ضعف آليات الكشف والتبليغ عن هذا النوع من السلوك داخل المكتبات الجامعية، فضلًا عن غياب أنظمة فعالة لرصد التلاعب، مما يؤدي إلى غموض أو عدم وضوح حول مدى انتشار هذه الظاهرة، وبالتالي تفاوت التقديرات بشأن خطورتها.

2. الإدخال الغير متعمد للبيانات الخاطئة من قبل الموظفين .

تشير نتائج الفقرة" الإدخال الغير متعمد للبيانات الخاطئة من قبل الموظفين " إلى أن المبحوثين يدركون بدرجة متوسطة وجود أخطاء غير متعمدة عند إدخال البيانات من قبل الموظفين، وهو ما يعكس احتمال حدوث هذه الأخطاء نتيجة لعوامل مثل نقص التدريب، ضغط العمل، أو ضعف في أنظمة التدقيق. ويتجلى هذا التصور في المتوسط الحسابي (2.80)، الذي يصنف ضمن درجة التبني المتوسطة.

ومع ذلك، فإن القيمة الاحتمالية (Sig = 0.070) التي تتجاوز عتبة الدلالة الإحصائية (0.05) تشير إلى عدم وجود اتفاق قوي بين آراء أفراد العينة، ما يعني أن درجة الوعي أو التقدير لانتشار هذه الأخطاء تختلف من شخص لآخر أو من مكتبة لأخرى.

يرجع الباحث سبب هذا التباين في الآراء إلى غياب أنظمة دقيقة لتوثيق الأخطاء البشرية أو آليات موحدة لرصدها وتحليلها، مما يجعل تقييم مدى حدوثها قائمًا على الانطباعات الذاتية والخبرة الشخصية، وليس على معطيات موضوعية يمكن الاعتماد عليها. هذا يشير إلى ضرورة تحسين أنظمة الرقابة والتدريب لتقليل مثل هذه الأخطاء وضمان جودة البيانات المدخلة.

3. التقادم التكنولوجي مثل الأجهزة والأنظمة المتقادمة.

تشير نتائج هذه الفقرة" التقادم التكنولوجي مثل الاجهزة والانظمة المتقادمة." إلى أن المبحوثين يدركون بدرجة متوسطة المخاطر المرتبطة باستخدام الأجهزة والأنظمة المتقادمة في المكتبات الجامعية، حيث بلغ المتوسط الحسابي (2.77)، وهو ما يعكس وعيًا نسبيًا بتأثير التقنيات القديمة على أمن وسلامة الأنظمة المعلوماتية، خصوصًا من حيث عدم قدرتها على مقاومة التهديدات الحديثة أو دعم التحديثات الأمنية المطلوبة.

إلا أن القيمة الاحتمالية(Sig = 0.061) ، التي تفوق مستوى الدلالة الإحصائية (0.05)، تدل على عدم وجود اتفاق قوي بين آراء المبحوثين، مما يشير إلى تباين في تقدير هذا التهديد.

يفسر الباحث هذا التباين بوجود تفاوت في البنية التحتية التقنية بين المكتبات الجامعية، فبعضها قد يكون مزودًا بتجهيزات حديثة، بينما تعاني أخرى من الاعتماد على أنظمة قديمة. كما قد يعود الاختلاف إلى تباين مستوى الوعي التقني بين الموظفين أو إلى غياب سياسات مؤسسية واضحة لتحديث البنية التكنولوجية بشكل دوري.

4. إتلاف البيانات المتعمد من قبل الموظفين.

تعكس نتائج الفقرة "اتلاف البيانات المتعمد من قبل الموظفين" إلى أن هناك إدراكًا متوسطًا لدى المبحوثين لاحتمالية قيام بعض الموظفين بإتلاف البيانات عن عمد، حيث بلغ المتوسط الحسابي (2.65). وتُعد هذه الفقرة دالة إحصائيًا (Sig = 0.002 < 0.05)، مما يدل على وجود اتفاق ملحوظ بين آراء أفراد العينة حول هذا النوع من التهديدات.

التفسير :تعكس هذه النتيجة وعيًا بوجود خطر داخلي قد يُمارس عن قصد من بعض الموظفين لأسباب مختلفة، مثل النزاعات الإدارية، أو ضعف الولاء المؤسسي، أو غياب الردع المؤسسي الفعّال. وتُظهر هذه القناعة أن التهديدات الداخلية لا تقل خطورة عن التهديدات الخارجية، خصوصًا إذا لم تُقابل بأنظمة رقابة فعّالة.

يرى الباحث أن هذه النتيجة تسلط الضوء على ضرورة تعزيز إجراءات الحوكمة والمساءلة داخل المكتبات الجامعية، من خلال تطبيق سياسات واضحة لتتبع العمليات وتسجيل الدخول والخروج من الأنظمة، مع فرض عقوبات واضحة على حالات التلاعب أو الإتلاف المتعمّد للبيانات. كما ينبغي رفع وعي الموظفين بالمسؤولية القانونية والأخلاقية المرتبطة بالتعامل مع المعلومات.

5. أخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين أثناء كتابة البرامج.

تشير نتائج هذه الفقرة " اخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين اثناء كتابة البرامج " إلى أن هناك إدراكًا متوسطًا من قبل المبحوثين بوجود خطر ناتج عن أخطاء فنية في البرمجة، حيث بلغ المتوسط الحسابي (2.62)، مع دلالة إحصائية معنوية .(Sig = 0.002 < 0.05) هذا يعكس اتفاقًا بين آراء أفراد العينة على أن أخطاء المبرمجين أثناء تطوير أو صيانة الأنظمة قد تشكل مصدرًا فعليًا لمخاطر أمنية.

يرى المبحوثون أن الأنظمة المعلوماتية بالمكتبات الجامعية قد تتأثر بأخطاء تقنية برمجية، مثل الثغرات الأمنية، أو ضعف التشفير، أو البرمجة غير المتوافقة مع المعايير الحديثة. هذه الأخطاء قد يتم استغلالها لاحقًا من قبل

مهاجمين، مما يجعل استقرار وأمن النظام عرضة للخطر، حتى لو لم يكن ذلك نتيجة هجوم مباشر، بل نتيجة إهمال أو ضعف في مراحل التطوير.

يفسر الباحث ذلك إلى قصور في تبني منهجيات تطوير آمنة للبرمجيات (Secure Software DevelopmentLifecycle)، وإخضاع الأنظمة لعمليات اختبار صارمة تشمل إختبارات الاختراق وفحص الكود المصدري قبل الإطلاق. كما ان عدم إشراف مهندسي نظم مؤهلون يؤدي إلى عدم الإلتزام بالمعايير الدولية لضمان سلامة واستقرار النظم المعلوماتية.

6. إتلاف البيانات غير متعمد من قبل الموظفين .

تبرز نتيجة الفقرة "إتلاف البيانات غير متعمد من قبل الموظفين " إلى أن أفراد العينة لديهم إدراك محدود لخطورة الإتلاف غير المقصود للبيانات من قبل الموظفين، وهو تهديد غالبًا ما ينتج عن ضعف التدريب، أو غياب الأدلة الإجرائية، أو غياب آليات الحفظ والنسخ الاحتياطي المنتظم. فرغم أن درجة التبني منخفضة، فإن الدلالة الإحصائية العالية تعكس وجود تصور مشترك ولو محدود بوجود هذا التهديد، مما يمنحه أهمية تستوجب المعالجة.

يرى الباحث أن إنخفاض متوسط التبني قد يعود إلى أن مثل هذه الحوادث لا يتم توثيقها أو الإبلاغ عنها بانتظام، ما يقلل من الوعي بحجم تأثيرها. ومع ذلك، فإن الدلالة الإحصائية توضح أنها قضية حقيقية تستحق الانتباه. لذا يوصي الباحث بضرورة إدراج هذا النوع من المخاطر في برامج التوعية والتدريب، مع تعزيز سياسات النسخ الاحتياطي التلقائي، وتوفير بروتوكولات واضحة للاسترجاع والتعامل مع الأخطاء البشرية.

3.3.6 مبدأ التوافر:

يعد مبدأ التوافر أحد الركائز الأساسية للأمن السيبراني، ويعني ضمان إتاحة المعلومات والأنظمة والخدمات المعلوماتية للمستفيدين في الوقت المناسب ودون إنقطاع، مع الحفاظ على إستمرارية العمل في حالات الهجمات السيبرانية، وتتجل أهمية هذا المبدأ على مستوى المكتبات في ضمان الوصول إلى فهارس البحث وقواعد البيانات والمستودعات الرقمية.

أ. الفرضية الفرعية الثالثة:

"مستوى التوافر عالي في المكتبات المركزية لجامعات الشرق الجزائري "

ب.عرض وتحليل الفقرات المتعلقة بالتوافر:

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (22) والذي يبين آراء أفراد عينة الدراسة لجميع فقرات المجال"التوافر"

جدول رقم (22) : المتوسط الحسابي وقيمة الاحتمال (Sig) لجميع فقرات المجال الثالث "التوافر"

التوافر		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحرافا لمعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول الى الخدمة).	التكرار	1	43	11	43	12	3.20	1.107	1.895-	0.061	متوسطة	2
	الوزن النسبي	0.9	39.1	10	39.1	10.9						
تفجير البريد الالكتروني (اغراق بريد المكتبة بالرسائل مما يؤدي الى توقفه عن العمل).	التكرار	0	40	11	51	8	3.25	1.033	2.491-	0.014	مرتفعة	1
	الوزن النسبي	0	36.4	10	46.4	7.3						
الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف.	التكرار	14	48	16	26	6	2.65	1.137	3.187-	0.002	متوسطة	4
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
اعطال اجهزة النظام الفنية.	التكرار	25	37	11	29	8	2.62	1.292	3.099	0.002	متوسطة	5
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
اعطال معدات الشبكة الفنية.	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	6
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
إنقطاع الإتصال بالأنترنت أو ضعف الإتصال بالشبكة بما يؤثر على إتاحة الخدمات الإلكترونية وإستمراريتها.	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	3
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
جميع فقرات المجال معا							2.84	0.56	5.923-	0.004	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يتبين أن المتوسط الحسابي لجميع فقرات المجال الثالث (التوافر) تساوي (2.84)، وقيمة t المحسوبة تساوي (-5.923) اما القيمة الاحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على أن مستوى التوافر متوسطة عند مستوى دلالة احصائية α 0.0 5

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب اراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي :

1. تفجير البريد الإلكتروني (إغراق بريد المكتبة بالرسائل مما يؤدي إلى توقفه عن العمل).

أظهرت نتائج الفقرة المتعلقة بـ"تفجير البريد الإلكتروني (إغراق بريد المكتبة بالرسائل مما يؤدي إلى توقفه عن العمل)" أن المتوسط الحسابي بلغ (3.25)، وهو ما يشير إلى درجة تبني مرتفعة لهذا التهديد، كما أن القيمة الاحتمالية (Sig = 0.014) كانت أقل من مستوى الدلالة (0.05)، ما يدل على دلالة إحصائية معنوية.

ويفسَّر الباحث هذه النتيجة إلى الاعتماد الواسع على البريد الإلكتروني في المعاملات اليومية، الأمر الذي يجعل أي خلل أو هجوم عليه أكثر وضوحًا وتأثيرًا لدى العاملين في المكتبات الجامعية ، الذي يُعد من أبرز التهديدات التي تؤثر سلبًا على توافر الخدمات الرقمية في بيئة المكتبة.

2. هجمات الحرمان من الخدمة.

أظهرت نتائج الفقرة المتعلقة بـ"هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول إلى الخدمة)" أن المتوسط الحسابي بلغ (3.20)، مما يشير إلى درجة تبنٍّ متوسطة لمدى خطورة هذا التهديد. ومع ذلك، فإن القيمة الاحتمالية (Sig = 0.061) جاءت أكبر من مستوى الدلالة المعتمد (0.05)، مما يعني أن النتائج غير دالة إحصائيًا. ويُفَسَّر الباحث بأن هذا النوع من الهجمات قد يؤثر على توافر الخدمات الرقمية، لكن تباين الآراء حال دون الوصول إلى إجماع قوي. كما يرى الباحث أن هذا التباين قد يُعزى إلى ندرة وقوع مثل هذه الهجمات بشكل مباشر في بيئة المكتبات الجامعية، وكذا إلى محدودية الفهم الفني لآليات الهجوم وتأثيراتها، ما يستدعي تعزيز برامج التوعية والتدريب حول تهديدات الحرمان من الخدمة وكيفية التعامل معها.

3. الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف.

أظهرت نتائج هذه الفقرة " الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف." أن المتوسط الحسابي بلغ (2.85)، ما يشير إلى درجة تبنٍ متوسطة لتهديد الكوارث الطبيعية على توافر البيانات والخدمات داخل المكتبات الجامعية.

ومع ذلك، فإن القيمة الاحتمالية (Sig = 0.203) تفوق مستوى الدلالة الإحصائية المعتمد (0.05)، مما يدل على أن النتائج غير دالة إحصائيًا، أي أن آراء أفراد العينة لم تتفق بشكل كبير بشأن هذا التهديد. كما يرى الباحث أن هذا التباين قد يُعزى إلى اختلاف البنية التحتية ومستوى الجاهزية بين المكتبات الجامعية،

بالإضافة إلى غياب أو محدودية خطط الطوارئ والاستجابة للكوارث، ما يؤدي إلى تباين في تصورات المبحوثين حول مدى تأثير الكوارث الطبيعية على الأمن السيبراني وتوافر الخدمات.

4. أعطال أجهزة النظام الفنية .

أظهرت نتائج هذه الفقرة " اعطال اجهزة النظام الفنية." أن المتوسط الحسابي بلغ (2.62)، مما يشير إلى تبنٍّ متوسط من طرف المبحوثين لاعتبار أعطال أجهزة النظام أحد مصادر تهديد التوافر داخل المكتبات الجامعية.

وقد جاءت القيمة الاحتمالية (Sig = 0.002) أقل من مستوى الدلالة الإحصائية المعتمد (0.05)، مما يدل على وجود اتفاق دال إحصائيًا بين أفراد العينة بشأن هذه المخاطر.

ويفسر الباحث هذا الاتفاق وعيًا بمدى اعتماد الخدمات المكتبية على سلامة وكفاءة الأجهزة التقنية المستخدمة، إذ إن تعطلها قد يؤدي إلى توقف الأنظمة أو الحد من إمكانية الوصول إلى الموارد الرقمية.

ويعزو الباحث هذه النتيجة إلى التجربة المباشرة التي قد يكون المبحوثون مروا بها نتيجة ضعف الصيانة أو تقادم المعدات، مما يبرز الحاجة إلى اعتماد سياسات صيانة وقائية وتحديث دوري للأجهزة لضمان استمرارية الخدمة والحد من الانقطاعات المفاجئة.

5. أعطال معدات الشبكة الفنية .

أشارت نتائج هذه الفقرة " اعطال معدات الشبكة الفنية " إلى أن المتوسط الحسابي بلغ (2.50)، مما يعكس مستوى تبنٍ منخفض لدى المبحوثين فيما يخص خطورة أعطال الشبكات الفنية على توافر خدمات المكتبة.

أظهرت النتائج دلالة إحصائية معتبرة، إذ بلغت القيمة الاحتمالية(Sig = 0.000) ، وهي أقل من مستوى الدلالة الإحصائية المعتمد (0.05)، ما يدل على وجود اتفاق بين المبحوثين حول وجود هذه المخاطر، وإن لم يُقدّر أثرها بدرجة عالية.

يُفسر الباحث هذا التباين بضعف الوعي الفني لدى العاملين بطبيعة عمل الشبكات وأهميتها الحيوية في ضمان استمرارية الوصول إلى الموارد والخدمات الرقمية؛ كما يُعزى انخفاض التقدير إلى الاعتماد الكبير على فرق الدعم التقني الخارجي، ما يجعل تأثير الأعطال أقل وضوحًا أو مباشرة من وجهة نظر الموظفين داخل المكتبات؛ ويؤكد ذلك أهمية تعزيز الثقافة التقنية الداخلية وربط العاملين بمفاهيم استمرارية الخدمة وسرعة الاستجابة للأعطال الشبكية ضمن بيئة العمل المكتبية.

4.3.6 مبدأ المخاطر العامة.

يرتبط مبدأ المخاطر العامة إرتباطا وثيقا بحوكمة المعلومات والأمن السيبراني ويقصد به التعرف على المخاطر المحتملة التي قد تؤثر في المعلومات والأنظمة المعلوماتية والخدمات الرقمية، وتحليلها وتقييمها، ثم إتخاذ التدابير الوقائية، وتشمل المخاطر العامة للأمن السيبراني في المكتبات الجامعية التهديدات التقنية والأخطاء البشرية والفنية.

أ. الفرضية الفرعية الرابعة:

"مستوى المخاطر العامة عالي في المكتبات المركزية لجامعات الشرق الجزائري"

ب.عرض وتحليل الفقرات المتعلقة بالمخاطر العامة.

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (23) تبين آراءأفراد عينة الدراسة لجميع فقرات المجال "المخاطر العامة".

جدول رقم (23): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجالالرابع "المخاطر العامة"

المخاطر العامة		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
قرصنة الهاتف (إجراء مكالمات مجانية؛ أو الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .)	التكرار	10	37	11	36	16	3.10	1.270	0.826-	0.411	متوسطة	4
	الوزن النسبي	9.1	33.6	10	32.7	14.5						
هجمات الانتحال مثل انتحال عنوانIP؛ او البريد الالكتروني؛ او موقع الويب؛ او هوية المتصل.	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	8
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).	التكرار	8	37	9	31	25	3.25	1.330	2.007-	0.047	مرتفعة	3
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
ديدان الحاسوب(قادرة على استنساخ نفسها تلقائيا).	التكرار	1	29	11	37	32	3.64	1.187	5.625-	0.000	مرتفعة	2
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
احصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله).	التكرار	14	47	12	24	13	2.77	1.261	1.890-	0.061	متوسطة	6
	الوزن النسبي	12.7	42.7	10.9	21.8	11.8						

برامج التجسس الالكتروني(برامج خفية تراقب استخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم).	التكرار	11	38	11	32	18	3.07	1.304	0.585-	0.560	متوسطة	5
	الوزن النسبي	10	34.5	10	29.1	16.4						
القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدأ بتدمير المعلومات).	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	7
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
هجمات الرسائل المزعجة او الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل.	التكرار	4	21	7	36	42	3.83	1.233	7.037-	0.000	مرتفعة	1
	الوزن النسبي	3.6	19.1	6.4	32.7	38.2						
جميع فقرات المجال معا							3.09	0.54	1.892-	0.061	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

توضح معطيات الجدول أعلاه أن المتوسط الحسابي لجميع فقرات المجال الرابع (المخاطر العامة) تساوي (2.84)، وقيمة t المحسوبة تساوي (-1.892) أما القيمة الإحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على أن مستوى المخاطر العامة متوسطة عند مستوى دلالة إحصائية α 0.05

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي :

1. **هجمات الرسائل المزعجة او الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل .**

جاءت هذه الفقرة " هجمات الرسائل المزعجة أو الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل."في المرتبة الأولى من حيث المتوسط الحسابي الذي بلغ (3.83).

كما أظهرت النتائج دلالة إحصائية قوية (Sig = 0.000 < 0.05) ؛ يعكس هذا المستوى المرتفع من التبني من قبل أفراد العينة وعيًا واضحًا لدى المبحوثين بخطورة الرسائل المزعجة أو غير المرغوب فيها، سواء عبر البريد الإلكتروني أو الرسائل القصيرة أو تطبيقات ومواقع التواصل الاجتماعي، لما لها من تأثير مباشر على توافر الخدمات وسرية المعلومات في البيئة الرقمية للمكتبات.

كما يرى الباحث أن هذا الإدراك قد يُعزى إلى الانتشار الواسع لهذا النوع من الهجمات وسهولة ملاحظتها وتكرار التعرض لها من قبل العاملين في المكتبات الجامعية، ما يجعلها من أكثر التهديدات وضوحًا وتأثيرًا في تصورات المبحوثين حول المخاطر السيبرانية، خاصة في ظل محدودية آليات تصفية المحتوى الرقمي في بعض المكتبات.

2. ديدان الحاسوب(قادرة على إستنساخ نفسها تلقائيا).

سجلت هذه الفقرة " ديدان الحاسوب(قادرة على استنساخ نفسها تلقائيا)."متوسطًا حسابيًا مرتفعًا بلغ (3.64)، مما يدل على درجة تبني مرتفعة من قبل أفراد العينة، كما أن القيمة الاحتمالية (Sig = 0.000) تشير إلى وجود دلالة إحصائية قوية عند مستوى دلالة 0.05. وتعكس هذه النتيجة إدراكًا متقدمًا بين المبحوثين لخطورة ديدان الحاسوب، التي تُعد من أكثر البرمجيات الخبيثة قدرة على الانتشار الذاتي، إذ لا تحتاج إلى تدخل المستخدم لتنتقل من جهاز إلى آخر، مما يجعلها تهديدًا مباشرًا لاستمرارية الخدمات الرقمية وسلامة الأنظمة.

ويرى الباحث أن هذا المستوى من الوعي يعكس فهمًا متزايدًا لآليات العدوى الرقمية في بيئة المكتبات، وربما يرتبط بتجارب سابقة أو بحملات توعوية داخل المؤسسات الجامعية. كما يبرز هذا الإدراك الحاجة إلى تعزيز استخدام البرمجيات الوقائية وتحديث أنظمة الحماية باستمرار، كجزء من استراتيجية أمن المعلومات الشاملة في المكتبات الجامعية.

3. فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).

أظهرت هذه الفقرة " فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب)." متوسطًا حسابيًا بلغ (3.25)، مما يشير إلى درجة تبني مرتفعة، في حين أن القيمة الاحتمالية (Sig = 0.047) أقل من 0.05، ما يدل على أن الفرق دال إحصائيًا عند مستوى الدلالة المعتمد. وتُبرز هذه النتيجة إدراكًا واسعًا من طرف المبحوثين لخطورة الفيروسات الرقمية، والتي تُعد من أكثر التهديدات السيبرانية شيوعًا وانتشارًا، نظرًا لقدرتها على التناسخ الذاتي والتسبب في تلف أو فقدان البيانات.

ويرى الباحث أن هذا الوعي يعكس تجارب متكررة واجهها المستخدمون في بيئة العمل، إلى جانب تأثير البرامج التوعوية والتدريبية التي تركز على أهمية حماية الأنظمة من هذه النوعية من البرمجيات الضارة. كما يشير إلى ضرورة استمرار تعزيز إجراءات الوقاية والتحديث الدوري لبرامج مكافحة الفيروسات داخل المكتبات الجامعية للحفاظ على سلامة البيانات الرقمية.

4. قرصنة الهاتف (إجراء مكالمات مجانية؛ او الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .

بلغ المتوسط الحسابي لهذه الفقرة" قرصنة الهاتف (اجراء مكالمات مجانية؛ او الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .)" (3.10)، إلى درجة تبني متوسطة، في حين أن القيمة الاحتمالية (Sig = 0.411) أكبر من 0.05، ما يعني أن الفرق غير دال إحصائيًا.

تدل هذه النتيجة على تباين ملحوظ في آراء المبحوثين حول خطورة قرصنة الهواتف، والتي قد تشمل إجراء مكالمات مجانية غير مشروعة، أو الوصول إلى معلومات حساسة، أو تعطيل خدمات الاتصالات.

ويرى الباحث أن هذا التباين قد يُعزى إلى محدودية الوعي التقني بهذه النوعية من التهديدات، خاصة في بيئة المكتبات الجامعية التي قد لا تعتمد بشكل مباشر على الاتصالات الهاتفية في تقديم خدماتها الرقمية. كما أن التركيز الأكبر في برامج التوعية قد يكون موجّهًا نحو الهجمات الأكثر شيوعًا، كالفيروسات والبريد الإلكتروني، مما يُضعف إدراك خطر قرصنة الهاتف لدى بعض الأفراد.

5. برامج التجسس الإلكتروني(برامج خفية تراقب إستخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم).

سجّلت هذه الفقرة " برامج التجسس الالكتروني(برامج خفية تراقب استخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم)." متوسطًا حسابيًا قدره (3.07)، ما يشير إلى درجة تبني متوسطة، بينما بلغت القيمة الاحتمالية(Sig = 0.560) ، وهي أعلى من 0.05، ما يدل على أن النتائج غير دالة إحصائيًا.

وتُشير هذه المعطيات إلى أن أفراد العينة يدركون بدرجة متوسطة وجود تهديد ناتج عن برامج التجسس الإلكترونية، والتي تتسلل خفيةً إلى الأجهزة لجمع بيانات المستخدمين دون علمهم. إلا أن هذا الإدراك غير متجانس بين المبحوثين، مما يفسر غياب الدلالة الإحصائية.

ويرى الباحث أن ضعف الإلمام بطبيعة هذه البرمجيات وآليات عملها، أو قلة التجارب المباشرة معها، قد يسهم في الحد من وعي العاملين بخطورتها. كما أن التركيز المؤسسي قد ينصب على تهديدات أخرى أكثر وضوحًا كالفيروسات وهجمات الرسائل المزعجة، ما يُقلل من إدراج برامج التجسس ضمن أولويات الأمن السيبراني في بيئة المكتبات.

6. أحصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله).

بلغ المتوسط الحسابي لهذه الفقرة "أحصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله)." (2.77)، مما يعكس درجة تبني متوسطة، في حين أن القيمة الاحتمالية (Sig = 0.061) كانت أعلى من 0.05، أي أن النتائج غير دالة إحصائيًا، يشير إلى وعي أفراد العينة بخطورة أحصنة طروادة ؛ البرامج الخبيثة التي تتخفى تحت مظهر برامج شرعية لتخريب النظام محدود أو متباين بين المبحوثين.

ويرى الباحث أن هذا التباين قد يرجع إلى عدم الفهم الكافي لآلية عمل هذه البرامج وكيفية تأثيرها، مما أدى إلى تفاوت في تقييم خطورتها بين العاملين في المكتبات الجامعية. كما يمكن أن يكون السبب ضعف التوعية التقنية المرتبطة بهذا النوع من البرمجيات الخبيثة.

7. **القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدا بتدمير المعلومات).**

بلغ المتوسط الحسابي لهذه الفقرة " القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدا بتدمير المعلومات)." (2.62)، ما يعكس درجة تبني متوسطة، مع وجود دلالة إحصائية واضحة حيث كانت القيمة الاحتمالية(Sig = 0.002 < 0.05) ، مما يشير إلى أن النتيجة دالة إحصائيًا.

ويعكس هذا الإدراك لدى المبحوثين وجود وعي حقيقي بخطورة البرمجيات التي تُفعّل بشكل مؤجل بهدف تدمير المعلومات أو تعطيل النظام، والمعروفة بـ"القنابل المعلوماتية."

يرى الباحث أن هذا الوعي رغم انخفاض متوسط التبني النسبي، يؤكد ضرورة تعزيز أنظمة الكشف المبكر والتدقيق الأمني، وذلك للحد من مخاطر هذه الهجمات التي قد تحدث بشكل مفاجئ وتسبب أضرارًا كبيرة.

8. **هجمات الإنتحال مثل إنتحال عنوانIP؛ أو البريد الالكتروني؛ أو موقع الويب؛ أو هوية المتصل .**

بلغ المتوسط الحسابي لهذه الفقرة " هجمات الانتحال مثل انتحال عنوانIP؛ او البريد الالكتروني؛ او موقع الويب؛ او هوية المتصل." (2.50)، مما يدل على درجة تبني منخفضة، مع وجود دلالة إحصائية قوية حيث كانت القيمة الاحتمالية(Sig = 0.000 < 0.05) ، أي أن النتيجة دالة إحصائيًا.

تشير النتائج إلى وجود ضعف واضح في إدراك المبحوثين لخطورة هجمات الانتحال، رغم أن التحليل الإحصائي يؤكد أهمية الموضوع.يرى الباحث أن هذا الضعف في الإدراك يعكس قلة الوعي أو قلة التعرض المباشر لهذا النوع من الهجمات، مما يستوجب زيادة التركيز على هذه المخاطر ضمن برامج التوعية السيبرانية لتطوير الفهم والقدرة على التصدي لها.

ثانيا: إختبار الفرضية الرئيسية الثالثة:

"مستوى مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي "

ثالثا: تحليل فقرات المحور الثالث؛ مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة.

تم استخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (24) والذي يبين آراء افراد عينة الدراسة لجميع مجالات المحور الثالث"مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية".

جدول رقم (24) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المحور الثالث "مستوى مخاطر الامن السيبراني"

الأبعاد	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	الترتيب
السـرية	2.64	0.56	-6.612	0.000	4
السـلامـة	2.69	0.58	-5.442	0.000	3
التـوافـر	2.84	0.56	-2.923	0.004	2
المخـاطر العـامة	3.09	0.54	-1.892	0.061	1
مستوى مخاطر الأمن السيبراني	2.84	0.51	-3.86	0.001	متوسطة

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

تشير نتائج الجدول رقم (24) إلى أن مستوى مخاطر الأمن السيبراني في المكتبات الجامعية محل الدراسة يُصنف ضمن الدرجة المتوسطة بمتوسط حسابي يبلغ (2.84) وقيمة دلالة إحصائية(Sig = 0.001) ، مما يعكس إدراكًا واضحًا بوجود تهديدات متعددة تؤثر على أمن نظم المعلومات بالمكتبات.

يتضح من ترتيب الأبعاد أن المخاطر العامة تتصدر قائمة المخاطر المدركة من قبل أفراد العينة بمتوسط حسابي (3.09)، تليها مخاطر التوافر، ثم السلامة والسرية على التوالي. بالرغم من أن بعد المخاطر العامة لم يظهر دلالة

إحصائية قوية، إلا أن متوسطه الأعلى يشير إلى وعي نسبي بأهمية هذه المخاطر. في المقابل، برزت دلالات إحصائية قوية لمخاطر التوافر والسلامة والسرية، مما يعكس اهتمامًا ملموسًا بهذه الجوانب ضمن نطاق الأمن السيبراني.

تدل هذه النتائج على وجود تفاوت في مستوى الوعي بين أبعاد الأمن السيبراني، الأمر الذي يستدعي تعزيز برامج التوعية والتدريب للموظفين في المكتبات الجامعية، بهدف رفع مستوى الاستجابة والجاهزية لمواجهة المخاطر السيبرانية بمختلف أنواعها وضمان حماية الموارد الرقمية والخدمات المقدمة.

4.6 أثر تطبيق حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري.

ترتبط حوكمة المعلومات إرتباطا وثيقا بمخاطر الأمن السيبراني، خصوصا أن حوكمة المعلومات أصبحت أحد الركائز الأساسية التي تعتمد عليها المؤسسات في إدارة مواردها في ظل تصاعد التهديدات السيبرانية، ويبرز أثرها من خلال تطبيق مبادئها.

يشمل المحور الرابع على 12 فقرة موزعة على 04 أبعاد نهدف من خلالها لمعرفة أثر حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات الجامعية محل الدراسة

أولا.الفرضية الرئيسية الرابعة:"أثر تطبيق حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي".

تنبثق عن الفرضيةأربع (04) فرضيات فرعيةتتحدد أبعاد أساسية.

1.4.6 السياسات الداخلية ومسؤولية الأفراد.

تعد السياسات الداخلية أحد العناصر الأساسية في حوكمة المعلومات، وترتبط إرتباطا وثيقا بمسؤولية الأفراد حيث تحدد واجبات ومسؤوليات الموظفين تجاه موارد المؤسسة في إطار تنظيمي يحدد الإجراءات والقواعد المنظمة.

أ. إختبار الفرضية الفرعية الأولى:

"تؤثر السياسات الداخلية ومسؤولية الأفراد على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري بصورة عالية".

ب. عرض وتحليل الفقرات المتعلقة بالسياسات الداخلية ومسؤولية الأفراد.

تم استخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (25) يبينآراء أفراد عينة الدراسة لجميع فقرات المجال الأول "السياسات الداخلية ومسؤولية الأفراد"

جدول رقم (25) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجال الأول " السياسات الداخلية ومسؤولية الأفراد

السياسات الداخلية ومسؤولية الافراد		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
عندما تكون المسؤوليات موزعة بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة. هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به، حيث يتم تطبيق تدابير تحكمية دقيقة تحد من عدد الأشخاص الذين لديهم إمكانية الوصول إلى البيانات الحساسة.	التكرار	14	46	13	24	13	2.33	1.264	5.581-	0.000	منخفضة	3
	الوزن النسبي	12.7	41.8	11.8	21.8	11.8						
توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها. هذا يسهم في تعزيز سلامة البيانات، حيث أن كل عملية تعديل تُراجع وتُعتمد من قبل المسؤولين المعنيين.	التكرار	24	41	10	27	8	2.58	1.273	3.444-	0.001	منخفضة	2
	الوزن النسبي	21.8	37.3	9.1	24.5	7.3						
وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية.	التكرار	14	47	12	24	13	2.77	1.261	1.890-	0.061	متوسطة	1
	الوزن النسبي	12.7	42.7	10.9	21.8	11.8						
جميع فقرات المجال معا							**2.56**	**0.75**	**3.582-**	**0.001**	**منخفضة**	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يتبين أن المتوسط الحسابي لجميع فقرات المجال الأول (السياسات الداخلية ومسؤولية الافراد) تساوي (2.56)، وقيمة t المحسوبة تساوي (-3.582)،أما القيمة الإحتمالية تساوي(0.000) وهي أقل من(

0.05) مما يدل على أن مستوى السياسات الداخلية ومسؤولية الأفراد متوسطة عند مستوى دلالة إحصائية 5 .α 0.0

تم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ وإستعادة البيانات بسرعة .

تشير نتائج الفقرة "وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية." إلى وجود إدراك متوسط لدى المبحوثين بأهمية تحديد المسؤوليات ضمن خطط الطوارئ، خصوصًا فيما يتعلق بإجراءات النسخ الاحتياطي واستعادة البيانات في حال التعرض لحوادث سيبرانية. ومع ذلك، فإن القيمة الإحصائية غير الدالة تعكس تباينًا واضحًا في آراء العينة، مما يدل على تفاوت في مستوى التطبيق أو المعرفة بالممارسات المتعلقة بإدارة الأزمات الرقمية.

يمكن يفسر الباحث هذا التباين بوجود فجوات في التدريب والتأهيل، وغياب سياسات واضحة لإسناد المهام والمسؤوليات أثناء الكوارث التقنية. وهو ما يستدعي تعزيز القدرات المؤسسية من خلال برامج تدريبية عملية وتوثيق خطط استجابة فعّالة ومحدثة في المكتبات الجامعية، بما يضمن الاستعداد الفعلي لمواجهة التهديدات السيبرانية واستمرارية الخدمات.

2. توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها.

تعكس نتيجة الفقرة " توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها. هذا يسهم في تعزيز سلامة البيانات، حيث أن كل عملية تعديل تُراجع وتُعتمد من قبل المسؤولين المعنيين." انخفاضًا في مستوى التبني العام لهذا المبدأ بين أفراد العينة، ورغم ذلك، تشير الدلالة الإحصائية إلى وجود وعي نسبي لدى بعض المبحوثين بأهمية توزيع المسؤوليات لضمان توثيق التعديلات ومراقبتها. هذا يدل على إدراك جزئي للدور الحيوي للرقابة المؤسسية في حماية سلامة البيانات من التلاعب أو التغيير غير المصرح به.

يفسر الباحث هذا الانخفاض إلى غياب سياسات وإجراءات مؤسسية مكتوبة تُنظم عملية تعديل البيانات واعتمادها، مما يؤدي إلى ضعف في تتبع العمليات وصعوبة ضمان الشفافية والمساءلة. لذا، يتطلب الأمر تطوير

آليات داخلية واضحة لتوزيع الصلاحيات وتوثيق كافة التعديلات ضمن نظام رقابي فعال يساهم في رفع مستوى سلامة البيانات داخل المكتبات الجامعية.

3. توزيع المسؤوليات بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة، هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به.

تشير نتائج الفقرة " عندما تكون المسؤوليات موزعة بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة. هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به، حيث يتم تطبيق تدابير تحكمية دقيقة تحد من عدد الأشخاص الذين لديهم إمكانية الوصول إلى البيانات الحساسة." إلى ضعف ملحوظ في إدراك أهمية التحكم في الوصول من خلال توزيع واضح للمسؤوليات، مع وجود دلالة إحصائية توضح أن هذا التفاوت في الآراء ذو أهمية. هذا يعكس نقصًا في تطبيق مفاهيم الحوكمة الأمنية التي تُعزز من وضوح المسؤوليات في العمليات.

يرى الباحث أن هذا الضعف يعكس قصورًا في نشر ثقافة الحوكمة الأمنية بين الأفراد، ويشير إلى اعتماد مفرط على الحلول التقنية دون وجود آليات واضحة للمساءلة والمسؤولية البشرية، مما يحد من فعالية الإجراءات الأمنية ويزيد من المخاطر المرتبطة بالوصول غير المصرح به.

4. تعامل المكتبة مع حالات الطوارئ وإستعادة البيانات بسرعة.

تعكس نتيجة الفقرة " المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية." وعيًا جزئيًا لدى المبحوثين بأهمية تحديد مسؤوليات واضحة في حالات الطوارئ، خاصة فيما يتعلق بإجراءات النسخ الاحتياطي والتعافي من الكوارث السيبرانية. التباين في الردود يشير إلى تفاوت في مدى تنفيذ هذه المسؤوليات بين المكتبات الجامعية محل الدراسة.

يفسر الباحث إلى أن هذا التفاوت يعكس اختلافًا في تطبيق خطط الطوارئ والإجراءات الوقائية، مما يبرز الحاجة إلى تعزيز التدريب العملي وتنظيم إجراءات واضحة لضمان سرعة وفعالية الاستجابة عند وقوع الحوادث السيبرانية.

2.4.6 التشريعات والمعايير العالمية

توفر هذه التشريعات والمعايير إطارًا قانونيًا وتنظيميًا يحدد مسؤوليات المؤسسات في حماية المعلومات، وضمان سرّيتها وسلامتها، كما تسهم في تعزيز حوكمة المعلومات والحد من مخاطر الأمن السيبيراني.

أ.إختبار الفرضية الفرعية الثانية:

"تؤثر التشريعات والمعايير العالمية على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري بصورة عالية"

ب.عرض وتحليل الفقرات المتعلقة التشريعات والمعاير العالمية.

تم استخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (26) يظهرآراء أفراد عينة الدراسة لجميع فقرات المجال الثاني"التشريعات والمعايير العالمية".

جدول رقم (26) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجال الثاني " التشريعات والمعايير العالمية "

التشريعات والمعايير العالمية		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
الامتثال للقوانين والتشريعات مثل GDPR وغيرها من المعايير العالمية يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة، ما يقلل من فرص التسريب أو الاختراق.	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	1
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
الامتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية مثل التشفير، التحقق متعدد العوامل، والتحديثات الأمنية الدورية، مما يحافظ على سلامة البيانات ويمنع التلاعب بها.	التكرار	25	37	11	29	8	2.62	1.292	3.099-	0.002	متوسطة	2
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
تتطلب التشريعات غالبًا خططًا للطوارئ واستمرارية الأعمال. الامتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الانقطاع غير المخطط له.	التكرار	49	35	9	16	1	1.95	1.095	10.01-1	0.000	منخفضة	3
	الوزن النسبي	44.5	31.8	8.2	14.5	9						

جميع فقرات المجال معا	2.47	0.72	7.649-	0.000	متوسطة

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يتبين أن المتوسط الحسابي لجميع فقرات المجال الثاني (التشريعات والمعايير العالمية) تساوي (2.47)، وقيمة t المحسوبة تساوي (-7.649)،أما القيمة الإحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على ان مستوى التشريعات والمعايير العالمية الافراد متوسطة عند مستوى دلالة احصائية 0.05 α

تم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب اراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي :

1.الإمتثال للقوانين والتشريعات يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة.

تشير نتيجة الفقرة " الإمتثال للقوانين والتشريعات مثل GDPR وغيرها من المعايير العالمية يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة، ما يقلل من فرص التسريب أو الاختراق " إلى وجود وعي نسبي لدى أفراد العينة بأهمية الامتثال للتشريعات العالمية المعنية بحماية البيانات، مثل اللائحة العامة لحماية البيانات .(GDPR) ومع ذلك، فإن عدم الدلالة الإحصائية يعكس تباينًا في مستوى التطبيق الفعلي بين المؤسسات الجامعية، وقد يدل على أن الالتزام بهذه المعايير لا يزال في طور الإدراك النظري دون ترجمة فعلية إلى سياسات تشغيلية واضحة.

يفسر الباحث هذا التفاوت بغياب استراتيجيات مؤسسية موحدة تُلزم المكتبات الجامعية باعتماد قوانين وتشريعات حماية البيانات كجزء من حوكمة المعلومات. ويوصى في هذا السياق بتكثيف حملات التوعية والتدريب حول أطر الامتثال القانوني، والعمل على إدماجها في السياسات العامة والأنظمة الداخلية، بما يعزز الممارسات الوقائية ويقلل من احتمالات التسريب أو الاختراق.

2.الإمتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية، التحقق متعدد العوامل، والتحديثات الأمنية الدورية.

تعكس نتيجة الفقرة " الإمتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية مثل التشفير، التحقق متعدد العوامل، والتحديثات الأمنية الدورية، مما يحافظ على سلامة البيانات ويمنع التلاعب بها". وعيًا متوسطًا لدى المبحوثين بأهمية الالتزام بالمعايير الأمنية التقنية، مع دلالة إحصائية قوية تؤكد وجود إدراك فعلي لدى

أفراد العينة بالدور الذي تلعبه هذه التدابير في حماية البيانات من التلاعب والاختراق. يشير ذلك إلى توجه إيجابي نسبي نحو تبني أدوات وتقنيات الحماية ضمن بيئة المكتبات الجامعية.

يري الباحث ان هذا الإدراك نتائج يعكس جهود سابقة في مجال التوعية التقنية، إلا أن متوسط التبني لا يزال أقل من المطلوب. وعليه، ينبغي تعزيز ثقافة أمن المعلومات عبر إلزامية تطبيق التدابير التقنية (مثل التشفير والمصادقة المتعددة) ضمن السياسات المؤسسية، وربطها بعمليات التدقيق والمتابعة الدورية لضمان الاستمرارية والفعالية.

7. تتطلب التشريعات غالبًا خططًا للطوارئ وإستمرارية الأعمال،الإمتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الإنقطاع غير المخطط له.

تعكس نتيجة الفقرة " تتطلب التشريعات غالبًا خططًا للطوارئ واستمرارية الأعمال. الامتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الانقطاع غير المخطط له."وعيًا متوسطًا لدى المبحوثين بأهمية الالتزام بالمعايير الأمنية التقنية، مع دلالة إحصائية قوية تؤكد وجود إدراك فعلي لدى أفراد العينة بالدور الذي تلعبه هذه التدابير في حماية البيانات من التلاعب والاختراق. يشير ذلك إلى توجه إيجابي نسبي نحو تبني أدوات وتقنيات الحماية ضمن بيئة المكتبات الجامعية.

يفسر الباحث مستوى هذا الإدراك نتائج جهود سابقة في مجال التوعية التقنية، إلا أن متوسط التبني لا يزال أقل من المطلوب. وعليه، ينبغي تعزيز ثقافة أمن المعلومات عبر إلزامية تطبيق التدابير التقنية (مثل التشفير والمصادقة المتعددة) ضمن السياسات المؤسسية، وربطها بعمليات التدقيق والمتابعة الدورية لضمان الاستمرارية والفعالية.

3.4.6كفاءة نظام دورة حياة البيانات

يمثل كفاءة نظام دورة حياة البيانات أحد المكونات الأساسية لحوكمة المعلومات، حيث تعكس مدى قدرة المؤسسة عل إدارة بياناتها بفاعلية منذ مرحلوة الإنشاء مرورا بالمعالجة والتخزين، يكتسب كفاءة نظام دورة حياة البيانات غي المكتبات الأكاديمية أهمية خاصة نظرًا لتعدد أنواع البيانات التي يتم التعامل معها مثل: البيانات الببليوجرافية، وبيانات المستفيدين، والبيانات البحثية، والموارد الرقمية. والنظام الكفئ بسهم في تحقيق السلامة والسرية والتوافر.

أ.إختبار الفرضية الفرعية الثالثة:

"تؤثر كفاءة نظام دورة حياة البيانات على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري بصورة عالية".

ب.عرض وتحليل الفقرات المتعلقة بكفاءة نظام دورة حياة البيانات.

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (27) يبين آراء أفراد عينة الدراسة لجميع فقرات المجال الثالث "كفاءة نظام دورة حياة البيانات".

جدول رقم (27) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجال الثالث "كفاءة نظام دورة حياة البيانات "

كفاءة نظام دورة حياة البيانات		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
سياسات الحفظ التي تشمل عمليات مراجعة وتدقيق دورية تساهم في الحفاظ على سلامة البيانات، حيث تتيح التعرف على أي تغييرات غير مصرح بها أو تلف قد يحدث للبيانات على المدى الطويل.	التكرار	14	43	11	30	12	2.85	1.265	1.282 -	0.203	متوسطة	1
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة التي قد تعيق الوصول الفعّال إلى المعلومات الهامة، مما يحسن من توافر البيانات الضرورية.	التكرار	25	37	11	29	8	2.62	1.292	3.099 -	0.002	متوسطة	2
	الوزن النسبي	22.7	33.6	10	26.4	7.3						
تطبيق سياسات الحفظ السليمة يضمن أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للاختراقات	التكرار	26	44	7	25	8	2.50	1.276	4.109 -	0.000	منخفضة	3
	الوزن النسبي	23.6	40	6.4	22.7	7.3						
جميع فقرات المجال معا							2.65	0.71	-5.086	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يتبين أن المتوسط الحسابي لجميع فقرات المجال الثاني (كفاءة نظام دورة حياة البيانات) تساوي (2.65)، وقيمة t المحسوبة تساوي (-5.086)،أما القيمة الإحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على أن مستوى كفاءة نظام دورة حياة البيانات. الأفراد متوسطة عند مستوى دلالة احصائية 0.05 α.

تم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي :

1. سياسات الحفظ .

تشير نتيجة الفقرة " سياسات الحفظ التي تشمل عمليات مراجعة وتدقيق دورية تساهم في الحفاظ على سلامة البيانات، حيث تتيح التعرف على أي تغييرات غير مصرح بها أو تلف قد يحدث للبيانات على المدى الطويل." إلى إدراك عام بأهمية وجود سياسات حفظ ومراجعة دورية للبيانات، لكنها لا تحمل دلالة إحصائية تؤكد الإجماع بين أفراد العينة. وهذا يرجعه الباحث الى التفاوت في تطبيق أو في المعرفة التفصيلية بهذه السياسات داخل المكتبات الجامعية.

ورغم أن السياسات الدورية للحفظ والتدقيق تعد عنصرًا أساسيًا في دورة حياة البيانات، فإن غياب الدلالة الإحصائية يعكس حاجة المؤسسات إلى مزيد من التوحيد والتفعيل لهذه الممارسات. وهذا ما يستلزم اعداد دلائل إجرائية موحدة لمراجعة البيانات بشكل دوري وتدريب العاملين على تطبيقها.

2. ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة.

تعكس نتيجة الفقرة " ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة التي قد تعيق الوصول الفعّال إلى المعلومات الهامة، مما يحسن من توافر البيانات الضرورية." وعيًا معتدلًا، لكن مستقرًا، لدى المبحوثين بأهمية التخلص من البيانات غير الضرورية لتحسين كفاءة الوصول إلى البيانات الفعلية. الدلالة الإحصائية تؤكد وجود إدراك واضح لهذه الممارسة ضمن بيئة العمل.

يري الباحثهذا المؤشر إيجابيًا، ويدل على فهم جيد لمبدأ "الحفظ الانتقائي" في إدارة البيانات. إلا أن ذلك يتطلب دعمه بسياسات حذف مؤتمتة ومراقبة دورية للبيانات المخزنة لضمان عدم تراكم المحتوى غير الضروري.

3. أن أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للإختراقات.

تُظهر نتيجة الفقرة "أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للاختراقات " وجود ضعف نسبي في وعي المبحوثين بمخاطر الاحتفاظ بالبيانات غير الضرورية، رغم أهمية هذا الجانب في خفض احتمالات الاختراق وتسرب المعلومات ومع ذلك، فإن وجود دلالة إحصائية يشير إلى وجود تفاوت حقيقي في الآراء يجب معالجته.

يفسر الباحث هذا الانخفاض في التبني إلى قصور في السياسات أو التكوين المهني المتعلق بإجراءات "الإتلاف الآمن" للبيانات. ينبغي للمكتبات الجامعية الاستثمار في تطوير سياسات واضحة لحذف البيانات وتدريب العاملين على تطبيقها بدقة، خاصة في ظل التزايد المستمر لحجم البيانات وتنوعها.

4.4.6فعالية وأمان عمليات الإستبعاد.

تظهر فعالية وأمان عمليات الإستبعاد في مدى كفاءة الإجراءات والسياسات المتبعة في التخلص من المعلومات والبيانات التي إنتهت صلاحية ومدة الحفظولم تعد ذات قيمة تشغيلية في المؤسسة.

أ. الفرضية الفرعية الرابعة:

"تؤثر فعالية وأمان عمليات الإستبعاد على مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري بصورة عالية"

ب. عرض وتحليل الفقرات المتعلقة فعالية وأمان عمليات الاستبعاد

تم إستخدام إختبار t للعينة الواحدة والجدول أدناهيوضح آراءأفراد عينة الدراسة لجميع فقرات المجال الرابع"فعالية وأمان عمليات الإستبعاد".

جدول رقم (28) : المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المجال الرابع " فعالية وامان عمليات الاستبعاد "

فعالية وأمان عمليات الاستبعاد		غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	درجة التبني	الترتيب
إجراءات الاستبعاد المطبقة بشكل صحيح تضمن أن البيانات الحساسة لا يمكن استعادتها بعد الحذف، مما يحميها من الاستخدام غير المشروع	التكرار	26	44	7	25	8	2.50	1.276	4.109-	0.000	منخفضة	3
	الوزن النسبي	23.6	40	6.4	22.7	7.3						

ويضمن بقاء المعلومات الخاصة تحت السيطرة الكاملة.											
تنفيذ عمليات الاستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية.	التكرار	14	48	16	26	6	2.65	1.137	3.187-	0.002	متوسطة	2
	الوزن النسبي	12.7	43.6	14.5	23.6	5.5						
الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة.	التكرار	14	43	11	30	12	2.85	1.265	1.282-	0.203	متوسطة	1
	الوزن النسبي	12.7	39.1	10	27.3	10.9						
جميع فقرات المجال معا							2.66	0.74	4.721-	0.000	متوسطة	

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

يوضح الجدول رقم (28)أن المتوسط الحسابي لجميع فقرات المجال الرابع "فعالية وأمان عمليات الإستبعاد"تساوي (2.66)، وقيمة t المحسوبة تساوي (-4.721) أما القيمة الإحتمالية تساوي(0.000) وهي أقل من(0.05) مما يدل على أن مستوى فعالية وأمان عمليات الإستبعاد . الأفراد متوسطة عند مستوى دلالة إحصائية 0.05 α.

تم تفسير نتيجة كل فقرة من فقرات هذا المجال وفقا لترتيب آراء المبحوثين في المكتبات الجامعية مجتمع الدراسة ترتيبا تنازليا حسب المتوسط الحسابي لكل فقرة كما يلي:

1. **الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة.**

تعكس هذه الفقرة " الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة."وجود تصور عام لدى المبحوثين حول أهمية الحذف المنتظم للبيانات غير الضرورية من أجل تحسين أداء النظام. إلا أن غياب الدلالة الإحصائية يشير إلى تباين في الآراء أو التباين في تطبيق هذا المفهوم عمليًا.

يري الباحث انهرغم وضوح العلاقة بين إزالة البيانات غير الضرورية وتحسين أداء الأنظمة، إلا أن غياب الدلالة الإحصائية يسلط الضوء على ضرورة وجود سياسات تضمن التطبيق المنهجي والدوري لهذه العمليات، بالإضافة إلى تعزيز التكوين في هذا الجانب.

2. تنفيذ عمليات الإستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية.

تشير نتائج الفقرة " تنفيذ عمليات الاستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية." إلى وجود وعي معتبر لدى أفراد العينة بأهمية تأمين عملية الحذف لحماية النظام من التهديدات السيبرانية الناتجة عن بقاء بيانات قديمة. الدلالة الإحصائية الإيجابية تؤكد على وضوح هذه الفكرة لدى المبحوثين.

يرى الباحث من خلال النتيجة المتوصل اليها وجود تطورًا نسبيًا في الفهم المتعلق بمخاطر البيانات المتبقية بعد الحذف، وهو ما يستدعي العمل على تعزيز إجراءات التحقق من الحذف الآمن مثل استخدام أدوات المسح النهائي (Data Wiping) ورفع كفاءة البرمجيات المستخدمة في هذا السياق.

3. الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة

نتائج الفقرة " الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة." تدل على ضعف في التبني العملي أو الفهم المتكامل للإجراءات التقنية التي تمنع استعادة البيانات بعد حذفها، رغم أهميتها البالغة. ومع ذلك، فإن الدلالة الإحصائية تشير إلى وجود اختلافات حقيقية في آراء المبحوثين يجب الوقوف عندها.

يفسر الباحث هذه النتيجة على أنها مؤشرًا لخلل واضح في تطبيق أدوات الحذف الآمن. لذا يُوصى بتوفير دورات تدريبية متخصصة للعاملين حول تقنيات التدمير النهائي للبيانات (مثل DOD Wipe، Degausser) وتعزيز ثقافة أمن المعلومات داخل المؤسسات.

ثانيا. إختبار الفرضية الرئيسية الرابعة:

"أثر تطبيق حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي".

ثالثا.تحليل جميع فقرات المحور الرابع :"حوكمة المعلومات واثرها على مخاطر الامن السيبراني"

تم إستخدام إختبار t للعينة الواحدة والنتائج المبينة في الجدول رقم (29) والذي يبين آراء أفراد عينة الدراسة لجميع مجالات المحور الرابع (حوكمة المعلومات واثرها على مخاطر الامن السيبرانيبالمكتبات الجامعية) .

جدول رقم (29): المتوسط الحسابي وقيمة الاحتمال (.Sig) لجميع فقرات المحور الرابع؛ حوكمة المعلومات واثرها على مخاطر الأمن السيبراني"

الأبعاد	المتوسط الحسابي	الانحراف المعياري	قيمة الاختبار T	القيمة الاحتمالية (.Sig)	الترتيب
السياسات الداخلية ومسؤولية الافراد	2.56	0.75	-6.068	0.000	3
التشريعات والمعايير العالمية	2.47	0.72	-7.649	0.000	4
كفاءة نظام دورة حياة البيانات	2.65	0.71	-5.086	0.000	2
فعالية وامان عمليات الاستبعاد	2.66	0.74	-4.721	0.000	1
أثر حوكمة المعلومات علىمخاطر الأمن السيبراني	2.58	0.49	-8.722	0.000	متوسطة

الارتباط دال احصائيا عند مستوى $\alpha \leq 0.05$.

تشير نتائج تحليل المحور الرابع إلى أن مستوى حوكمة المعلومات في المكتبات الجامعية محل الدراسة يُصنّف ضمن المستوى المتوسط، حيث تراوحت المتوسطات الحسابية بين (2.47) و(2.66)، مع دلالة إحصائية قوية لجميع الأبعاد عند مستوى معنوية .(Sig 0.000) وقد تبيّن أن بُعد "فعالية وأمان عمليات الاستبعاد" جاء في المرتبة الأولى، مما يعكس اهتمامًا نسبيًا بالجوانب الفنية المرتبطة بحذف البيانات وتأمينها. بينما جاء بعد "التشريعات والمعايير العالمية" في المرتبة الأخيرة، ما يدل على ضعف واضح في الامتثال للمعايير الدولية ذات الصلة بحوكمة المعلومات وحماية البيانات.

ومن خلال استقراء هذه النتائج، يُمكن الاستنتاج أن هناك بوادر تبنٍ لبعض ممارسات الحوكمة، خصوصًا في ما يتعلق بالجوانب التقنية، في حين لا تزال الأبعاد التنظيمية والمؤسسية، مثل السياسات الداخلية والتشريعات، بحاجة إلى دعم وتعزيز. كما تُظهر النتائج إدراكًا عامًا لأهمية حوكمة المعلومات في الحد من مخاطر الأمن السيبراني، إلا أن هذا الإدراك لم يتحول بعد إلى ممارسات متكاملة أو سياسات موحّدة على مستوى جميع المكتبات الجامعية.

وعليه، توصي الدراسة بضرورة تبني إطار حوكمة معلومات شامل يتضمن سياسات مكتوبة، وتكوينات مهنية منتظمة، وآليات تقييم دورية، مع مراعاة التكامل مع المعايير والتشريعات العالمية، بما يُعزز من قدرة المكتبات الجامعية على مواجهة التحديات السيبرانية بفعالية أكبر.

5.6 الفروقات ذات الدلالة الإحصائية حول مستوى مخاطر الأمن السيبراني بالمكتبات المركزية وفق متغيرات الدراسة.

أولا. الفرضية الخامسة الرئيسية:

"لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى لمتغيرات (الجنس ، العمر، المؤهل العلمي، الخبرة المهنية)".

قام الباحثبدراسة الفروق في إتجاهات المبحوثين نحو متغيرات الدراسة بالإستناد إلى المتغيرات الشخصية والوظيفية، وسنسعى من خلال ذلك إلى إختبار الفرضية التالية:

H0: لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغيرات(الجنس ، الرتبة ، المستوى العلمي، الخبرة المهنية، جامعةالعمل)

سيتم إختبار التجانس عند إختبار الفرضيات بالنسبة للمتغيرات الشخصية والوظيفية فيما يلي، حيث سيتم إختبار الفرضية الرئيسية من خلال الفرضيات الفرعية التالية:H0 و H1 .

1.5.6 الفروقات ذات الدلالة الإحصائية حول مستوى مخاطر الأمن السيبراني وفق متغير الجنس.

نتائج إختبار الفرضية الرئيسية الخامسة لإختبار الفروق حول مستوى مخاطر الامن السيبراني حسب إجابات المبحوثين، وفقا لمتغير الجنس.

الفرضية الصفرية H0:" لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى لمتغير الجنس"

الفرضية البديلة H1: "توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في بالمكتبات محمل الدراسة تعزى متغير الجنس."

بما أنه يمكن تقسيم العينة إلى عينتين مستقلتين (ذكور، إناث)، فإننا نستخدم إختبار T ، للعينات المستقلة Independent sample T- test ، وذلك لتوضيح دلالة الفروق بين إجابات أفراد عينة الدراسة حسب الجنس، وجاءت النتائج كما يلي:

جدول رقم (30): إختبار الفروق حول مستوى مخاطر الأمن السيبراني تعزى لمتغير الجنس

المجال	الجنس	العدد	المتوسط الحسابي	الإنحراف المعياري	متوسط الخطأ المعياري
مخاطر الأمن السيبراني	ذكر	39	2.569	0.541	0.086
	انثى	71	2.712	0.581	0.069

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

بناء على إخبار الفروق حول مستوى مخاطر الأمن السيبراني، حسب المقياس قدر المتوسط الحسابي لفئة الذكور 2.569 بمعدل إنحراف معياري 0.541، في حين بلغ لمتوسط الحسابي لفئة الإناث ب2.712 وإنحراف معياري بلغ 0.581.

جدول رقم (31) : نتائج إختبار الفروقات Test-t للعينات المستقلة حول مستوى مخاطر الأمن السيبراني حسب متغير الجنس

		إختبار Levene لتجانس التباين		إختبار Test-t لتجانس المتوسطات (Test-e pour egalite des moyennes)				
		F	Sig	T	درجة الحرية	Sig (bilaterale)	فرق المتوسطات	فرق الخطأ المعياري
مخاطر الامن السيبراني	فرضية تجانس التباين	0.731	0.394	1.259	108	0.211	-0.142	0.113
	فرضية عدم تجانس التباين			1.286	83.285	0.202	-0.142	0.110

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

بناء على إختبار Leveneللتجانس وجدنا مستوى المعنوية(0.394) وهي أكبر من مستوى الدلالة المعتمد 0.05، مما يعني أن هناك تجانسا في التباين بين الذكور والإناث، وبالتالي تحقق شرط التجانس وهو أحد الشروط الأساسية لإختبار الفروق لذا سوف نعتمد على نتائج إختبار

(Independent sample T- test) لمقارنة المتوسطات.

خلال النتائج الموضحة في الجدول رقم(31) يتضح أن مستوى الدلالة المحسوب بلغ (0.211) وهي أكبر من مستوى الدلالة (0.05)، وهذا ما يشير إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة(0.05) في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات محل الدراسة تعزى لمتغير الجنس.

وبذلك نقبل الفرضية الصفرية التي تنص على عدم وجود فروق ذات دلالة إحصائية للإجابات مبحوثي الدراسة حول مستوى مخاطر الأمن السيبراني تعزى لمتغير الجنس في المكتبات محل الدراسة.

2.5.6 الفروقات ذات الدلالة الإحصائية حول مستوى مخاطر الأمن السيبراني وفق متغير الرتبة.

نتائج إختبار الفرضية الرئيسية الخامسة لإختبار الفروق حول مستوى مخاطر الأمن السيبراني حسب إجابات المبحوثين، وفقا لمتغير الرتبة.

الفرضية الصفرية H0:"لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى لمتغير الرتبة".

الفرضية البديلةH1:"توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في بالمكتبات محل الدراسة تعزى متغير الرتبة".

لإختبار هذه الفرضية تم إستخدام تحليل التباين الأحادي(One Way ANOVA)بداية بإختبار شرط التجانس كما يلي:

جدول رقم (32): إختبار تجانس التباين متغير الرتبة

إحصائيات Levene	درجة الحريةddl1	درجة الحريةddl2	مستوى الدلالة
0.594	**5**	104	0.705

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

من خلال النتائج الموضحة في جدول إختبار تجانس التباين(Levene) ، يتضح أن قيمة مستوى الدلالة الإحصائية (**Sig. = 0.705**)، وهي قيمة أكبر من مستوى الدلالة المعتمد (**0.05**) وهذا مايحقق شرط التجانس لإختبار الفروق تبعا لمتغير الرتبة، وكانت نتائج تحليل التباين الاحادي لاختبار الفروق الرتبة كما يلي:

جدول رقم (33) : نتائج تحليل التباين لاختبار الفروق في اتجاهات المبحوثين حول مستوى مخاطر الامن السيبراني تعزى لمتغير الرتبة

مخاطر الأمن السيبراني	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمةFالمحوسبة	مستوى الدلالة
	بين المجموعات	3,830	5	0.766	2.528	0.033
	داخل المجموعات	31,514	104	0.303		
	المجموع	35,344	109			

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

من خلال النتائج الموضحة في الجدول رقم (33) يتضح أن قيمة (F) المحسوبة بلغت (2.528) والدالة الإحصائية (0.033). وهو أقل من مستوى الدلالة المعتمد (0.05)، وهذا ما يدل على وجود أثر لمتغير الرتبة على إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة، وبالتالي نرفض الفرضية الصفرية ونقبل الفرضية البديلة التي تنص على وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات الجامعية محل الدراسة تعزى لمتغير الرتبة.

لتدعيم نتائج تحليل التباين الأحادي، تم إستخدام إختبار (LSD) للمقارنات البعدية بين فئات المستوى العلميكما هو موضح في الجدول التالي:

جدول رقم (34) : نتائج اختبارLSD للفروق في الإجابات المبحوثين حول مستوى مخاطر الامن السيبراني بالمكتبات الجامعية محل الدراسة حسب متغير الرتبة.

المستوى العلمي (I)	المستوى العلمي (J)	الفروق في المتوسطات(I–J)	الخطأ المعياري	مستوى الدلالة	مجالات الثقة عند نسبة95%	
					الحد الأدنى	الحد الاعلى

رئيس محافظي المكتبات الجامعية	محافظ المكتبات الجامعية	0.07047	0.24397	0.773	-0.4133	0.5543
	ملحق بالمكتبات من المستوى اثاني	-0.14470	0.22595	0.523	-0.5928	0.3034
	ملحق بالمكتبات من المستوى الاول	-0.46114*	0.22256	0.041	-0.9025	-0.0198
	مساعد بالمكتبات الجامعية	-0.16458	0.22871	0.473	-0.6181	0.2890
	عون تقني بالمكتبات الجامعية	-0.39625	0.23391	0.093	-0.8601	0.0676
محافظ المكتبات الجامعية	رئيس محافظي المكتبات الجامعية	-0.07047	0.24397	0.773	-0.5543	0.4133
	ملحق بالمكتبات من المستوى اثاني	-0.21517	0.18660	0.252	-0.5852	0.1549
	ملحق بالمكتبات من المستوى الاول	-0.53161*	0.18248	0.004	-0.8935	-0.1697
	مساعد بالمكتبات الجامعية	-0.23505	0.18993	0.219	-0.6117	0.1416
	عون تقني بالمكتبات الجامعية	-0.46672*	0.19616	0.019	-0.8557	-0.0777
ملحق بالمكتبات من المستوى اثاني	رئيس محافظي المكتبات الجامعية	0.14470	0.22595	0.523	-0.3034	0.5928
	محافظ المكتبات الجامعية	0.21517	0.18660	0.252	-0.1549	0.5852

	ملحق بالمكتبات من المستوى الاول	-0.31644*	0.15757	0.047	-0.6289	-0.0040
	مساعد بالمكتبات الجامعية	-0.01988	0.16615	0.905	-0.3493	0.3096
	عون تقني بالمكتبات الجامعية	-0.25155	0.17323	0.149	-0.5951	0.0920
ملحق بالمكتبات من المستوى الاول	رئيس محافظي المكتبات الجامعية	0.46114*	0.22256	0.041	0.0198	0.9025
	محافظ المكتبات الجامعية	0.53161*	0.18248	0.004	0.1697	0.8935
	ملحق بالمكتبات من المستوى الثاني	0.31644*	0.15757	0.047	0.0040	0.6289
	مساعد بالمكتبات الجامعية	0.29656	0.16151	0.069	-0.0237	0.6168
	عون تقني بالمكتبات الجامعية	0.06489	0.16879	0.701	-0.2698	0.3996
مساعد بالمكتبات الجامعية	رئيس محافظي المكتبات الجامعية	0.16458	0.22871	0.473	-0.2890	0.6181
	محافظ المكتبات الجامعية	0.23505	0.18993	,219	-,1416	,6117
	ملحق	0,01988	0.16615	0.905	-0.3096	0.3493

	بالمكتبات من المستوى اثاني					
	ملحق بالمكتبات من المستوى الاول	-0.29656	0.16151	0.069	-0.6168	0.0237
	عون تقني بالمكتبات الجامعية	-0.23167	0.17682	0.193	-0.5823	0.1190
عون تقني بالمكتبات الجامعية	رئيس محافظي المكتبات الجامعية	0.39625	0.23391	0.093	-0.0676	0.8601
	محافظ المكتبات الجامعية	0.46672*	0.19616	0.019	0.0777	0.8557
	ملحق بالمكتبات من المستوى اثاني	0.25155	0.17323	0.149	-0.0920	0.5951
	ملحق بالمكتبات من المستوى الاول	-0.06489	0.16879	0.701	-0.3996	0.2698
	مساعد بالمكتبات الجامعية	0.23167	0.17682	0.193	-0.1190	0.5823

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تشير نتائج المقارنات البعدية بإستخدام إختباري (LSD) إلى أن الفروق في إتجاهات المبحوثين حولمستوى مخاطر الأمن السيبراني حسب متغير الرتبة ليست عامة بين جميع الفئات الوظيفية، وإنما تقتصر على بعض الثنائيات المحددة فقط.

فقد أظهرت نتائج إختبار (LSD) وجود فروق ذات دلالة إحصائية عند مستوى (0.05) بين فئة ملحق بالمكتبات من المستوى الأول وكل من رئيس محافظي المكتبات الجامعية ومحافظي المكتبات الجامعية وملحق بالمكتبات من المستوى الثاني، حيث جاءت الفروق لصالح فئة ملحق بالمكتبات من المستوى الأول، وهو ما يدل على إختلاف مستوى إدراك مخاطر الأمن السيبراني لدى هذه الفئة مقارنة ببعض الفئات الوظيفية الأعلى أو الأدنى منها وظيفيًا. كما كشفت النتائج عن وجود فرق دال إحصائيًا بين فئة عون تقني بالمكتبات الجامعية ومحافظي المكتبات الجامعية لصالح الفئة التقنية، وهو ما يعكس تباينًا في طبيعة التعامل مع الأنظمة الرقمية بين الفئات الوظيفية ذات الطابع التقني والإداري.

ويمكن تفسير هذه النتيجة في ضوء طبيعة الأدوار الوظيفية داخل المكتبات الجامعية، حيث تُعد فئة **ملحق بالمكتبات من المستوى الأول** من أكثر الفئات احتكاكًا المباشر بالأنظمة الإلكترونية وقواعد البيانات والخدمات الرقمية اليومية، مقارنة بالفئات الإدارية العليا التي يغلب على مهامها الطابع الإشرافي والتنظيمي. كما أن الفئات التقنية قد تمتلك وعيًا عمليًا أعلى بالمخاطر السيبرانية نتيجة تعاملها المباشر مع البنية التحتية التقنية، وهو ما يفسر الفروق الجزئية التي ظهرت بينها وبين بعض الفئات الأخرى. ومن ثمّ فإن متغير **الرتبة** يبدو أكثر تفسيرًا للفروق في إدراك مخاطر الأمن السيبراني مقارنة بمتغير الخبرة المهنية، إلا أن هذا التأثير يظل محصورًا في نطاق ضيق ولا يعكس تباينًا شاملًا بين جميع الفئات الوظيفية.

وعليه، يمكن القول إن نتائج المقارنات المتعددة تؤكد أن الوعي بمخاطر الأمن السيبراني داخل المكتبات الجامعية محل الدراسة يتأثر جزئيًا بطبيعة **الرتبة** ومهامها الفعلية أكثر من تأثره بالمستوى الوظيفي الشكلي أو سنوات الخبرة، وهو ما يبرز أهمية تبني مقاربات تدريبية وتوعوية موجهة حسب الأدوار الوظيفية، بدل الاقتصار على برامج توعوية عامة موحدة.

وتؤكد هذه النتيجة أن بناء ثقافة أمن سيبراني فعّالة داخل المكتبات الجامعية يتطلب مراعاة الخصوصية الوظيفية في تصميم برامج التكوين والتوعية، بما ينسجم مع طبيعة المهام والمسؤوليات التقنية والإدارية لكل فئة وظيفية.

3.5.6 الفروقات ذات الدلالة الإحصائية حول مستوى مخاطر الأمن السيبراني وفق متغير المستوى العلمي.

نتائج إختبار الفرضية الرئيسية الخامسة لإختبار الفروق حول مستوى مخاطر الأمن السيبراني حسب إجابات المبحوثين، وفق متغير المستوى العلمي.

الفرضية الصفرية H0:"لا توجد فروق ذات دلالة إحصائية في إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى لمتغير المستوى العلمي".

الفرضية البديلة H1": توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى متغير المستوى العلمي".

لإختبار هذه الفرضية تم إستخدام تحليل التباين الأحادي(One Way ANOVA) بداية بإختبار شرط التجانس كما يلي:

جدول رقم (35): إختبار تجانس التباين وفقمتغير المستوى**العلمي**

إحصائيات Levene	درجة الحرية1ddl	درجة الحرية2ddl	مستوى الدلالة
1.182	4	105	0.368

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

بناء على إختبار التجانس وجدنا مستوى الحرية (0.368)، وهو أكبر من مستوى المعتمد (0.05)، وهذا مايحقق شرط التجانس لإختبار الفروق تبعا لمتغير المستوى العلمي.

وكانت نتائج تحليل التباين الاحادي لإختبار الفروق المستوى العلمي كما يلي:

جدول رقم (36) : نتائج تحليل التباين One Way ANOVA لإختبار الفروق في اتجاهات المبحوثين حول مستوى مخاطر الامن السيبراني تعزى لمتغير المستوى**العلمي**

مخاطر الامن السيبراني	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمةFالمحوسبة	مستوى الدلالة
	بين المجموعات	2.387	4	0.597	1.901	0.116
	داخل المجموعات	32.957	105	0.314		
	المجموع	35.344	109			

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

من خلال النتائج الموضحة في الجدول رقم (36) يتضح أن قيمة (F) المحسوبة بلغت (1.901) والدالة الإحصائية (0.116)وهو أكبر من مستوى الدلالة المعتمد (0.05)، وهذا ما يدل على عدم وجود أثر لمتغير المستوى العلمي على إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة.

وبالتالي نرفض الفرضية البديلة ونقبل الفرضية الصفرية التي تنص على عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات الجامعية محل الدراسة تعزى لمتغير المستوى العلمي.

ولتدعيم نتائج تحليل التباين الأحادي، تم إستخدام إختبار (LSD) للمقارنات البعدية بين فئات المستوى العلميكما هو موضح في الجدول التالي:

جدول رقم (37) : نتائج اختبارLSD للفروق في الإجابات المبحوثين حول مستوى مخاطر الامن السيبراني بالمكتبات الجامعية محل الدراسة حسب متغير المستوى العلمي.

المستوى العلمي (I)	المستوى العلمي (J)	الفروق في المتوسطات(I–J)	الخطأ المعياري	مستوى الدلالة	مجالات الثقة عند نسبة95%	
					الحد الادنى	الحد الاعلى
السنة الثالثة ثانوي	دراسات تطبيقية	–0.06793	0.15172	0.655	–0.3688	0.2329
	ليسانس	0.12348	0.15693	0.433	–0.1877	0.4347
	ماستر	0.25456	0.16378	0.123	–0.0702	0.5793
	دكتوراه	0.43041	0.23957	0.075	–0.0446	0.9054
دراسات تطبيقية	السنة الثالثة ثانوي	0.06793	0.15172	0.655	–0.2329	0.3688
	ليسانس	0.19141	0.15012	0.205	–0.1062	0.4891
	ماستر	0.32249*	0.15726	0.043	0.0107	0.6343
	دكتوراه	0.49833*	0.23516	0.036	0.0320	0.9646

ليسانس	السنة الثالثة ثانوي	-0.12348	0.15693	0.433	-0.4347	0.1877
	دراسات تطبيقية	-0.19141	0.15012	0.205	-0.4891	0.1062
	ماستر	0.13108	0.16229	0.421	-0.1907	0.4529
	دكتوراه	0.30692	0.23856	0.201	-0.1661	0.7799
ماستر	السنة الثالثة ثانوي	-0.25456	0.16378	0.123	-0.5793	0.0702
	دراسات تطبيقية	-0.32249*	0.15726	0.043	-0.6343	-0.0107
	ليسانس	-0.13108	0.16229	0.421	-0.4529	0.1907
	دكتوراه	0.17585	0.24312	0.471	-0.3062	0.6579
دكتوراه	السنة الثالثة ثانوي	-0.43041	0.23957	0.075	-0.9054	0.0446
	دراسات تطبيقية	-0.49833*	0.23516	0.036	-0.9646	-0.0320
	ليسانس	-0.30692	0.23856	0.201	-0.7799	0.1661
	ماستر	-0.17585	0.24312	0.471	-0.6579	0.3062

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

أظهر إختبار LSD للمقارنات الثنائية أن هناك فروقات معنوية عند مستوى 0.05 بين فئة الدراسات التطبيقية والفئة السنة الثالثة ثانوي، وكذلك بين فئة الدراسات التطبيقية ودرجة الماستر، حيث كانت فئة الدراسات التطبيقية تقيم المخاطر السيبرانية بمستوى أعلى من الفئتين الأخريين.

وبناءً على ذلك، يمكن القول إن الفروقات بين فئات المؤهل العلمي في إدراك مخاطر الأمن السيبراني جزئية وليست شاملة لجميع الفئات، مما يعكس الحاجة إلى برامج تدريبية مكثفة ومستهدفة للفئات ذات المستوى التعليمي الأقل لرفع مستوى الوعي بالمخاطر السيبرانية داخل المكتبات الجامعية.

4.5.6 الفروقات ذات الدلالة الإحصائية حول مستوى مخاطر الأمن السيبراني وفق متغيرات الخبرة المهنية.

نتائج إختبار الفرضية الرئيسية الخامسة لإختبار الفروق حول مستوى مخاطر الأمن السيبراني حسب إجابات المبحوثين، وفقا لمتغيرات الخبرة المهنية.

الفرضية الصفرية H0:"لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى لمتغيرات الخبرة المهنية".

الفرضية البديلة H1: "توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات محل الدراسة تعزى متغيرات الخبرة المهنية".

لإختبار هذه الفرضية تم إستخدام تحليل التباين الأحادي (One Way ANOVA) بداية بإختبار شرط التجانس كما يلي:

جدول رقم (38): إختبار تجانس التباين وفق متغير الخبرة المهنية

إحصائيات Levene	درجة الحريةddl1	درجة الحريةddl2	مستوى الدلالة
0.629	4	105	0.643

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

بناء على إختبار التجانس وجدنا مستوى الحرية (0.643)، وهو أكبر من مستوى المعتمد (0.05)، وهذا مايحقق شرط التجانس لإختبار الفروق تبعا لمتغير الخبرة المهنية.وكانت نتائج تحليل التباين الأحادي لإختبار فروق الخبرة المهنية كمايلي:

جدول رقم (39) : نتائج تحليل التباين One Way ANOVA لإختبار الفروق في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغير الخبرة المهنية

مخاطر الامن	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمةFالمحوسبة	مستوى الدلالة

السيبراني	بين المجموعات	0.306	4	0.076	0.229	0.922
	داخل المجموعات	35.038	105	0.334		
	المجموع	35.344	109			

المصدر: من إعداد الباحث بالإعتماد على مخرجات SPSS

من خلال النتائج الموضحة في الجدول رقم (39) يتضح أن قيمة (F) المحسوبة بلغت (0.229) والدالة الإحصائية (0.922)، وهو أكبر من مستوى الدلالة المعتمد (0.05)، وهذا ما يدل على عدم وجود أثر لمتغير الخبرة المهنية على إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة.

وبالتالي نرفض الفرضية البديلة ونقبل الفرضية الصفرية التي تنص على عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (0.05) في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات الجامعية محل الدراسة تعزى لمتغير الخبرة المهنية. كما يشير إرتفاع مستوى الدلالة إلى:

- تجانس إدراك المخاطر بين مختلف فئات الخبرة
- فعالية السياسات أو برامج التوعية الموحدة داخل المكتبات الجامعية محل الدراسة

وللتحقق من طبيعة الفروق بين فئات الخبرة المهنية، تم إستخدام إختبار المقارنات البعدية(LSD) ، كما هو موضح في الجدول رقم (40)، وذلك بهدف التأكد من عدم وجود فروق ذات دلالة إحصائية بين أي ثنائية من ثنائيات الخبرة المهنية في إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة.

جدول رقم (40): نتائج إختبار (LSD) للمقارنات البعدية للفروق في إجابات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة حسب متغير الخبرة المهنية.

المؤهل العلمي (I)	الخبرة المهنية (J)	الفروق في المتوسطات(I-J)	الخطأ المعياري	مستوى الدلالة	مجالات الثقة عند نسبة95%	
					الحد الادنى	الحد الاعلى
أقلمن5سنوات	من5الى 10 سنوات	0.13681	0.26605	0.608	-0.3907	0.6644
	من 10الى15سنة	0.17980	0.25765	0.487	-0.3311	0.6907
	من	0.07121	0.25699	0.782	-0.4384	0.5808

	15الى20سنة					
	اكثر من20سنة	0.15998	0.27052	0.556	–0.3764	0.6964
من5الى 10 سنوات	اقلمن5سنوات	–0.13681	0.26605	0.608	–0.6644	0.3907
	من 10الى15سنة	0.04299	0.16104	0.790	–0.2763	0.3623
	من 15الى20سنة	–0.06560	0.15999	0.683	–0.3828	0.2516
	اكثر من20سنة	0.02317	0.18092	0.898	–0.3356	0.3819
من 10الى15سنة	اقل من5سنوات	-0.17980	0.25765	0.487	-0.6907	0.3311
	من5الى 10 سنوات	-0.04299	0.16104	0.790	-0.3623	0.2763
	من 15الى20سنة	-0.10859	,14558	0.457	-0.3972	0.1801
	اكثر من20سنة	-0.01982	0.16831	0.906	-0.3535	0.3139
من 15الى20سنة	اقل من5سنوات	-0.07121	0.25699	0.782	-0.5808	0.4384
	من5الى 10 سنوات	0.06560	0.15999	0.683	-0.2516	0.3828
	من 10الى15سنة	0.10859	0.14558	0.457	-0.1801	0.3972
	اكثر من20سنة	0.08877	0.16731	0.597	-0.2430	0.4205
أكثر من20سنة	اقل من5سنوات	-0.15998	0.27052	0.556	-0.6964	0.3764
	من5الى 10 سنوات	-0.02317	0.18092	0.898	-0.3819	0.3356
	من 10الى15سنة	0.01982	0.16831	0.906	-0.3139	0.3535
	من 15الى20سنة	-0.08877	0.16731	0.597	-0.4205	0.2430

المصدر: من إعداد الباحث بالاعتماد على مخرجاتSPSS

تظهر نتائج المقارنات البعدية بإستخدام إختبار (LSD) عدم وجود فروق ذات دلالة إحصائية بين أي ثنائية من فئات الخبرة المهنية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني، حيث جاءت جميع القيم الاحتمالية (Sig) أكبر من مستوى الدلالة المعتمد(0.05) ، كما أن فواصل الثقة عند مستوى (95%) احتوت على الصفر في جميع المقارنات الثنائية. ويؤكد ذلك أن الفروق الظاهرية بين المتوسطات، وإن وُجدت من حيث القيمة العددية، فإنها لا ترقى إلى مستوى الدلالة الإحصائية، بما يعكس تقاربًا حقيقيًا في إدراك مخاطر الأمن السيبراني بين مختلف فئات الخبرة المهنية.

من منظور تحليلي نستنتج بأن الخبرة المهنية، بوصفها متغيرًا زمنيًا تراكميًا، لا تُشكّل عاملًا فارقًا في تشكيل اتجاهات العاملين نحو مخاطر الأمن السيبراني داخل بيئة المكتبات الجامعية، خاصة في ظل إعتماد هذه المؤسسات على نظم تقنية موحدة، وسياسات أمن معلومات مركزية، وإجراءات تشغيل قياسية تُطبّق على جميع العاملين دون تمييز. كما يوحي غياب الفروق الثنائية بأن مصادر الوعي بالمخاطر السيبرانية باتت مؤسسية الطابع، ناتجة عن التدريب المنظم والتوجيه الإداري والثقافة التنظيمية السائدة، أكثر من كونها ناتجة عن الخبرة الفردية المتراكمة.

تسهم نتائج إختبار (LSD) هنا في تدعيم ما خلص إليه تحليل التباين الأحادي، إذ تؤكد أن عدم دلالة الفروق لا يقتصر على المقارنة الكلية بين المجموعات، بل يمتد ليشمل جميع المقارنات الثنائية الممكنة بين فئات الخبرة المهنية. وعليه يمكن اعتبار هذا التقارب مؤشرًا على مستوى من النضج المؤسسي في إدارة المخاطر السيبرانية داخل المكتبات الجامعية محل الدراسة، حيث يتم تعميم الوعي الأمني بصورة أفقية بين العاملين، بما يقلل من أثر الفروق الفردية المرتبطة بسنوات الخبرة، ويعزز من إتساق الاتجاهات تجاه قضايا الأمن السيبراني.

وعليه إن بناء الوعي بمخاطر الأمن السيبراني في المؤسسات الأكاديمية ينبغي أن يُفهم في إطار مقاربات تنظيمية شمولية، لا في إطار متغيرات فردية معزولة كطول الخبرة المهنية.

5.5.6 الفروقات ذات الدلالة الإحصائية حول مستو مخاطر الأمن السيبراني حسب متغير الجامعة.

نتائج إختبار الفرضية الرئيسية الخامسة لإختبار الفروق حول مستوى مخاطر الأمن السيبراني حسب إجابات المبحوثين، وفقا لمتغيرجامعة العمل .

الفرضية الصفرية H0:"لا توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات محل الدراسة تعزى لمتغير جامعة العمل".

الفرضية البديلة H1": توجد فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني في المكتبات محمل الدراسة تعزى متغير جامعة العمل".

لإختبار هذه الفرضية تم إستخدام تحليل التباين الاحادي (One Way ANOVA)بداية بإختبار شرط التجانس كما يلي:

جدول رقم (41) : إختبار تجانس التباين وفق متغير جامعة العمل.

إحصائيات Levene	درجة الحرية1ddl	درجة الحرية2ddl	مستوى الدلالة
2,785	15	94	0.001

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

يبين جدول رقم (41) نتائج إختبار (Levene)لتجانس التباين تبعًا لمتغير جامعة العمل، حيث بلغت القيمة الإحتمالية للاختبار المعتمد على المتوسط(0.001) ، وهي قيمة أقل من مستوى الدلالة(0.05) ، دالة إحصائيًاوهذايشير عدم تحقق شرط تجانس التباين إلى وجود اختلافات في تشتت إستجابات المبحوثين بين الجامعات محل الدراسة.

وجودعددكبير من الفئات درجة الحرية (ddl1=15)يزيد من إحتمال عدم تجانس التباين، ويعكستنوع السياقات المؤسسية بين الجامعات،إختلاف البنى التحتية الرقمية وسياسات الأمن السيبيراني.

بسبب عدم تحقق شرط تجانس التباين، تم إعتماد إختبار Welch ANOVA بوصفه بديلًا مناسبًا لتحليل التباين الأحادي، لما يتمتع به من قدرة على التعامل مع التباينات غير المتجانسة والحفاظ على دقةالمقارنة بين المتوسطات.

جدول رقم (42) : نتائج اختبارWelch ANOVAلاختبار الفروق في اتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغير جامعة العمل

إحصائيات Welch	درجة الحرية1ddl	درجة الحرية2ddl	مستوى الدلالة

20,977	20,977	15	5,002

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

يبين جدول رقم (42) إختبارات التباين المتينة (Robust Tests of Equality of Means) أن قيمة اختبار Welch بلغت (F = 5.002) عند مستوى دلالة(Sig = 0.000) ، وهي قيمة دالة إحصائيًا عند مستوى(0.05) ، مما يدل على وجود فروق ذات دلالة إحصائية في اتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني بالمكتبات الجامعية محل الدراسة تعزى لمتغير جامعة العمل. وبناءً على ذلك، تم رفض الفرضية الصفرية وقبول الفرضية البديلة.

ونظرًا لدلالة نتائج إختبارWelch، تم إجراء اختبار المقارنات البعدية (Games-Howell) لتحديد مصدر الفروق بين الجامعات.

جدول رقم (43):نتائج إختبار Games-Howell للمقارنات البعدية للفروق في اتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغير جامعة العمل.

Comparaisons multiples :

Variable dépendante: 3االمحورا_متوسط

Games-Howell

جامعة العمل (I)	جامعة العمل (J)	Différence moyenne (I-J)	Erreur standard	Sig.	Intervalle de confiance à 95 % Borne inférieure	Borne supérieure
تبسة	1باتنة	-,47227	,40915	,984	-3,1965	2,2520
	1سطيف	-,58436	,41667	,950	-3,2376	2,0688
	2سطيف	-,41488	,46125	,999	-2,8590	2,0293
	جامعة الامير	-,29439	,43798	1,000	-2,8362	2,2474
	جيجل	-,63797	,43486	,942	-3,1855	1,9096
	منتوري	-,44928	,43324	,995	-2,9893	2,0907
	الطارف	-,52728	,59193	,999	-3,9773	2,9227
	ام البواقي	-,34997	,40763	,998	-3,0900	2,3900
	سوق اهراس	-,34821	,48095	1,000	-3,4121	2,7157
	عنابة	-,91220	,39121	,645	-3,8681	2,0437
	قالمة	-,58274	,42860	,961	-3,1764	2,0109
	المسيلة	-,29911	,47810	1,000	-2,7535	2,1552
	رقلة	,03001	,46945	1,000	-2,4471	2,5071
	البرج	-1,09970	,40943	,514	-3,8283	1,6289
	3قسنطينة	-,10119	,47578	1,000	-2,7645	2,5621

باتنة1	تبسة	,47227	,40915	,984	-2,2520	3,1965
	سطيف1	-,11210	,18686	1,000	-,8303	,6062
	سطيف2	,05739	,27213	1,000	-1,0681	1,1829
	جامعة الامير	,17787	,23051	1,000	-,8654	1,2211
	جيجل	-,16570	,22452	1,000	-1,1338	,8024
	منتوري	,02299	,22136	1,000	-,8452	,8912
	الطارف	-,05501	,46009	1,000	-4,4791	4,3690
	ام البواقي	,12229	,16573	1,000	-,5215	,7661
	سوق اهراس	,12405	,30433	1,000	-5,7228	5,9709
	عنابة	-,43994	,11980	,130	-,9647	,0848
	قالمة	-,11047	,21214	1,000	-1,0988	,8778
	المسيلة	,17316	,29981	1,000	-1,2043	1,5506
	رقلة	,50228	,28582	,876	-,8700	1,8745
	البرج	-,62744	,17012	,115	-1,3518	,0969
	قسنطينة3	,37108	,29610	,967	-1,9688	2,7110
سطيف1	تبسة	,58436	,41667	,950	-2,0688	3,2376
	باتنة1	,11210	,18686	1,000	-,6062	,8303
	سطيف2	,16948	,28331	1,000	-,9770	1,3160
	جامعة الامير	,28997	,24361	,993	-,7655	1,3454
	جيجل	-,05360	,23795	1,000	-1,0439	,9367
	منتوري	,13508	,23497	1,000	-,7716	1,0417
	الطارف	,05708	,46679	1,000	-4,1800	4,2942
	ام البواقي	,23439	,18351	,993	-,4718	,9405
	سوق اهراس	,23615	,31437	,998	-4,6377	5,1100
	عنابة	-,32784	,14340	,639	-,9315	,2758
	قالمة	,00163	,22631	1,000	-,9966	,9999
	المسيلة	,28526	,30999	,999	-1,0945	1,6650
	رقلة	,61437	,29648	,747	-,7532	1,9820
	البرج	-,51534	,18748	,387	-1,2826	,2519
	قسنطينة3	,48317	,30641	,903	-1,7033	2,6696
سطيف2	تبسة	,41488	,46125	,999	-2,0293	2,8590
	باتنة1	-,05739	,27213	1,000	-1,1829	1,0681
	سطيف1	-,16948	,28331	1,000	-1,3160	,9770
	جامعة الامير	,12049	,31382	1,000	-1,1646	1,4056
	جيجل	-,22309	,30945	1,000	-1,4750	1,0288
	منتوري	-,03440	,30716	1,000	-1,2471	1,1783
	الطارف	-,11240	,50698	1,000	-3,6608	3,4360
	ام البواقي	,06491	,26984	1,000	-1,0564	1,1862
	سوق اهراس	,06667	,37144	1,000	-2,8019	2,9352
	عنابة	-,49732	,24434	,766	-1,5960	,6014
	قالمة	-,16786	,30059	1,000	-1,4150	1,0792

	المسيلة	,11577	,36774	1,000	-1,3967	1,6282
	رقلة	,44489	,35642	,991	-1,0461	1,9359
	البرج	-,68482	,27256	,514	-1,8268	,4572
	3قسنطينة	,31369	,36472	,999	-1,5879	2,2153
جامعة الامير	تبسة	,29439	,43798	1,000	-2,2474	2,8362
	1باتنة	-,17787	,23051	1,000	-1,2211	,8654
	1سطيف	-,28997	,24361	,993	-1,3454	,7655
	2سطيف	-,12049	,31382	1,000	-1,4056	1,1646
	جيجل	-,34357	,27357	,990	-1,5203	,8332
	منتوري	-,15489	,27098	1,000	-1,2758	,9660
	الطارف	-,23289	,48592	1,000	-4,0933	3,6275
	ام البواقي	-,05558	,22781	1,000	-1,0969	,9858
	سوق اهراس	-,05382	,34213	1,000	-3,6244	3,5168
	عنابة	-,61781	,19693	,339	-1,7079	,4723
	قالمة	-,28834	,26351	,996	-1,4732	,8966
	المسيلة	-,00471	,33811	1,000	-1,4708	1,4614
	رقلة	,32440	,32576	,999	-1,1271	1,7759
	البرج	-,80531	,23102	,191	-1,8769	,2663
	3قسنطينة	,19320	,33482	1,000	-1,8305	2,2169
جيجل	تبسة	,63797	,43486	,942	-1,9096	3,1855
	1باتنة	,16570	,22452	1,000	-,8024	1,1338
	1سطيف	,05360	,23795	1,000	-,9367	1,0439
	2سطيف	,22309	,30945	1,000	-1,0288	1,4750
	جامعة الامير	,34357	,27357	,990	-,8332	1,5203
	منتوري	,18869	,26591	1,000	-,8828	1,2602
	الطارف	,11069	,48311	1,000	-3,7894	4,0107
	ام البواقي	,28799	,22175	,986	-,6757	1,2517
	سوق اهراس	,28975	,33812	,996	-3,3796	3,9591
	عنابة	-,27423	,18989	,956	-1,2469	,6984
	قالمة	,05523	,25829	1,000	-1,0800	1,1905
	المسيلة	,33886	,33405	,999	-1,1027	1,7805
	رقلة	,66798	,32155	,747	-,7575	2,0935
	البرج	-,46173	,22505	,760	-1,4597	,5362
	3قسنطينة	,53678	,33073	,899	-1,4854	2,5590
منتوري	تبسة	,44928	,43324	,995	-2,0907	2,9893
	1باتنة	-,02299	,22136	1,000	-,8912	,8452
	1سطيف	-,13508	,23497	1,000	-1,0417	,7716
	2سطيف	,03440	,30716	1,000	-1,1783	1,2471
	جامعة الامير	,15489	,27098	1,000	-,9660	1,2758
	جيجل	-,18869	,26591	1,000	-1,2602	,8828
	الطارف	-,07800	,48164	1,000	-3,9885	3,8325

	ام البواقي	,09931	,21854	1,000	-,7606	,9593
	سوق اهراس	,10107	,33603	1,000	-3,5790	3,7812
	عنابة	-,46292	,18614	,532	-1,2608	,3349
	قالمة	-,13346	,25554	1,000	-1,2023	,9354
	المسيلة	,15017	,33193	1,000	-1,2605	1,5608
	رقلة	,47929	,31935	,958	-,9118	1,8704
	البرج	-,65042	,22189	,300	-1,5484	,2476
	قسنطينة3	,34809	,32859	,993	-1,6478	2,3440
الطارف	تبسة	,52728	,59193	,999	-2,9227	3,9773
	باتنة1	,05501	,46009	1,000	-4,3690	4,4791
	سطيف1	-,05708	,46679	1,000	-4,2942	4,1800
	سطيف2	,11240	,50698	1,000	-3,4360	3,6608
	جامعة الامير	,23289	,48592	1,000	-3,6275	4,0933
	جيجل	-,11069	,48311	1,000	-4,0107	3,7894
	منتوري	,07800	,48164	1,000	-3,8325	3,9885
	ام البواقي	,17731	,45875	1,000	-4,2876	4,6422
	سوق اهراس	,17907	,52498	1,000	-3,8218	4,1799
	عنابة	-,38492	,44422	,996	-5,3810	4,6112
	قالمة	-,05546	,47748	1,000	-4,0749	3,9639
	المسيلة	,22817	,52237	1,000	-3,2089	3,6652
	رقلة	,55729	,51446	,989	-2,9617	4,0763
	البرج	-,57242	,46035	,963	-4,9964	3,8516
	قسنطينة3	,42609	,52025	,999	-3,2303	4,0825
ام البواقي	تبسة	,34997	,40763	,998	-2,3900	3,0900
	باتنة1	-,12229	,16573	1,000	-,7661	,5215
	سطيف1	-,23439	,18351	,993	-,9405	,4718
	سطيف2	-,06491	,26984	1,000	-1,1862	1,0564
	جامعة الامير	,05558	,22781	1,000	-,9858	1,0969
	جيجل	-,28799	,22175	,986	-1,2517	,6757
	منتوري	-,09931	,21854	1,000	-,9593	,7606
	الطارف	-,17731	,45875	1,000	-4,6422	4,2876
	سوق اهراس	,00176	,30229	1,000	-6,0934	6,0969
	عنابة	-,56223*	,11452	,024	-1,0638	-,0607
	قالمة	-,23277	,20920	,995	-1,2200	,7544
	المسيلة	,05087	,29774	1,000	-1,3266	1,4283
	رقلة	,37998	,28364	,976	-,9940	1,7539
	البرج	-,74973*	,16644	,037	-1,4645	-,0349
	قسنطينة3	,24878	,29400	,998	-2,1284	2,6260
سوق اهراس	تبسة	,34821	,48095	1,000	-2,7157	3,4121
	باتنة1	-,12405	,30433	1,000	-5,9709	5,7228
	سطيف1	-,23615	,31437	,998	-5,1100	4,6377

	2سطيف	-,06667	,37144	1,000	-2,9352	2,8019
	جامعة الامير	,05382	,34213	1,000	-3,5168	3,6244
	جيجل	-,28975	,33812	,996	-3,9591	3,3796
	منتوري	-,10107	,33603	1,000	-3,7812	3,5790
	الطارف	-,17907	,52498	1,000	-4,1799	3,8218
	ام البواقي	-,00176	,30229	1,000	-6,0969	6,0934
	عنابة	-,56399	,27976	,769	-11,7056	10,5777
	قالمة	-,23452	,33003	,999	-4,2875	3,8185
	المسيلة	,04911	,39217	1,000	-2,6859	2,7841
	رقلة	,37822	,38158	,993	-2,4940	3,2504
	البرج	-,75149	,30472	,651	-6,6083	5,1053
	3قسنطينة	,24702	,38934	1,000	-3,0652	3,5592
عنابة	تبسة	,91220	,39121	,645	-2,0437	3,8681
	1باتنة	,43994	,11980	,130	-,0848	,9647
	1سطيف	,32784	,14340	,639	-,2758	,9315
	2سطيف	,49732	,24434	,766	-,6014	1,5960
	جامعة الامير	,61781	,19693	,339	-,4723	1,7079
	جيجل	,27423	,18989	,956	-,6984	1,2469
	منتوري	,46292	,18614	,532	-,3349	1,2608
	الطارف	,38492	,44422	,996	-4,6112	5,3810
	ام البواقي	,56223*	,11452	,024	,0607	1,0638
	سوق اهراس	,56399	,27976	,769	-10,5777	11,7056
	قالمة	,32946	,17508	,811	-,7592	1,4181
	المسيلة	,61310	,27483	,671	-,7946	2,0208
	رقلة	,94221	,25950	,225	-,4942	2,3786
	البرج	-,18750	,12078	,917	-,9385	,5635
	3قسنطينة	,81101	,27078	,495	-2,2344	3,8565
قالمة	تبسة	,58274	,42860	,961	-2,0109	3,1764
	1باتنة	,11047	,21214	1,000	-,8778	1,0988
	1سطيف	-,00163	,22631	1,000	-,9999	,9966
	2سطيف	,16786	,30059	1,000	-1,0792	1,4150
	جامعة الامير	,28834	,26351	,996	-,8966	1,4732
	جيجل	-,05523	,25829	1,000	-1,1905	1,0800
	منتوري	,13346	,25554	1,000	-,9354	1,2023
	الطارف	,05546	,47748	1,000	-3,9639	4,0749
	ام البواقي	,23277	,20920	,995	-,7544	1,2200
	سوق اهراس	,23452	,33003	,999	-3,8185	4,2875
	عنابة	-,32946	,17508	,811	-1,4181	,7592
	المسيلة	,28363	,32586	1,000	-1,1612	1,7285
	رقلة	,61275	,31304	,801	-,8210	2,0465
	البرج	-,51696	,21270	,575	-1,5424	,5085

	قسنطينة3	,48155	,32245	,929	-1,6209	2,5840
المسيلة	تبسة	,29911	,47810	1,000	-2,1552	2,7535
	باتنة1	-,17316	,29981	1,000	-1,5506	1,2043
	سطيف1	-,28526	,30999	,999	-1,6650	1,0945
	سطيف2	-,11577	,36774	1,000	-1,6282	1,3967
	جامعة الامير	,00471	,33811	1,000	-1,4614	1,4708
	جيجل	-,33886	,33405	,999	-1,7805	1,1027
	منتوري	-,15017	,33193	1,000	-1,5608	1,2605
	الطارف	-,22817	,52237	1,000	-3,6652	3,2089
	ام البواقي	-,05087	,29774	1,000	-1,4283	1,3266
	سوق اهراس	-,04911	,39217	1,000	-2,7841	2,6859
	عنابة	-,61310	,27483	,671	-2,0208	,7946
	قالمة	-,28363	,32586	1,000	-1,7285	1,1612
	رقلة	,32912	,37798	1,000	-1,2914	1,9497
	البرج	-,80060	,30020	,460	-2,1909	,5897
	قسنطينة3	,19792	,38582	1,000	-1,7670	2,1629
رقلة	تبسة	-,03001	,46945	1,000	-2,5071	2,4471
	باتنة1	-,50228	,28582	,876	-1,8745	,8700
	سطيف1	-,61437	,29648	,747	-1,9820	,7532
	سطيف2	-,44489	,35642	,991	-1,9359	1,0461
	جامعة الامير	-,32440	,32576	,999	-1,7759	1,1271
	جيجل	-,66798	,32155	,747	-2,0935	,7575
	منتوري	-,47929	,31935	,958	-1,8704	,9118
	الطارف	-,55729	,51446	,989	-4,0763	2,9617
	ام البواقي	-,37998	,28364	,976	-1,7539	,9940
	سوق اهراس	-,37822	,38158	,993	-3,2504	2,4940
	عنابة	-,94221	,25950	,225	-2,3786	,4942
	قالمة	-,61275	,31304	,801	-2,0465	,8210
	المسيلة	-,32912	,37798	1,000	-1,9497	1,2914
	البرج	-1,12971	,28623	,128	-2,5171	,2576
	قسنطينة3	-,13120	,37505	1,000	-2,1206	1,8582
البرج	تبسة	1,09970	,40943	,514	-1,6289	3,8283
	باتنة1	,62744	,17012	,115	-,0969	1,3518
	سطيف1	,51534	,18748	,387	-,2519	1,2826
	سطيف2	,68482	,27256	,514	-,4572	1,8268
	جامعة الامير	,80531	,23102	,191	-,2663	1,8769
	جيجل	,46173	,22505	,760	-,5362	1,4597
	منتوري	,65042	,22189	,300	-,2476	1,5484
	الطارف	,57242	,46035	,963	-3,8516	4,9964
	ام البواقي	,74973*	,16644	,037	,0349	1,4645
	سوق اهراس	,75149	,30472	,651	-5,1053	6,6083

	عنابة	,18750	,12078	,917	-,5635	,9385
	قالمة	,51696	,21270	,575	-,5085	1,5424
	المسيلة	,80060	,30020	,460	-,5897	2,1909
	رقلة	1,12971	,28623	,128	-,2576	2,5171
	3قسنطينة	,99851	,29649	,366	-1,3575	3,3545
3قسنطينة	تبسة	,10119	,47578	1,000	-2,5621	2,7645
	1باتنة	-,37108	,29610	,967	-2,7110	1,9688
	1سطيف	-,48317	,30641	,903	-2,6696	1,7033
	2سطيف	-,31369	,36472	,999	-2,2153	1,5879
	جامعة الامير	-,19320	,33482	1,000	-2,2169	1,8305
	جيجل	-,53678	,33073	,899	-2,5590	1,4854
	منتوري	-,34809	,32859	,993	-2,3440	1,6478
	الطارف	-,42609	,52025	,999	-4,0825	3,2303
	ام البواقي	-,24878	,29400	,998	-2,6260	2,1284
	سوق اهراس	-,24702	,38934	1,000	-3,5592	3,0652
	عنابة	-,81101	,27078	,495	-3,8565	2,2344
	قالمة	-,48155	,32245	,929	-2,5840	1,6209
	المسيلة	-,19792	,38582	1,000	-2,1629	1,7670
	رقلة	,13120	,37505	1,000	-1,8582	2,1206
	البرج	-,99851	,29649	,366	-3,3545	1,3575

*. La différence moyenne est significative au niveau 0.05.

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

يبين جدول رقم (43) المقارنات البعدية بإستخدام إختبار Games-Howell وجود فروق ذات دلالة إحصائية في إتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغير جامعة العمل، حيث ظهرت هذه الفروق بين جامعة أم البواقي وكل من جامعة عنابة وجامعة البرج، وكانت الفروق لصالح الجامعتين الأخيرتين. في المقابل، لم تُسجل فروق ذات دلالة إحصائية بين باقي الجامعات محل الدراسة، مما يدل على أن أثر متغير جامعة العمل كان جزئيًا ومحصورًا في بعض الجامعات دون غيرها.

يمكن تفسير هذه الفروق الجزئية بوجود تباين في مستوى الجاهزية الرقمية، أو إختلاف في سياسات أمن المعلومات، أو في برامج التكوين والتوعية بالأمن السيبراني المعتمدة داخل بعض الجامعات دون غيرها. كما قد يعكس ذلك تفاوتًا في البنية التحتية التقنية أو في درجة الاحتكاك اليومي بالأنظمة الرقمية داخل المكتبات الجامعية، الأمر الذي يؤثر مباشرة في إدراك العاملين لمخاطر الأمن السيبراني.

تم قبول الفرضية البديلة، حيث وُجدت فروق ذات دلالة إحصائية في اتجاهات المبحوثين حول مستوى مخاطر الأمن السيبراني تعزى لمتغير جامعة العمل، إلا أن هذه الفروق كانت محدودة ولم تشمل جميع الجامعات محل الدراسة.

6.6 مناقشة نتائج الدراسة

في هذا المبحث سيتم التركيز على تفسير نتائج إختبار فرضيات الدراسة، حيث يتم من خلاله تقييم مدى صحة الفرضيات بناءا على النتائج الإحصائية، وعرض النتائج العامة لكل محور وأبعده.

- **تفسير نتائج إختبار الفرضية الأولى.**

"مستوى وعي أخصائي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبيراني بالمكتبات المركزية لجامعات الشرق الجزائري منخفض".

كشفت الدراسة فيما يتعلق بالمحور الأول الخاص بوعي أخصائيّي المعلومات بحوكمة المعلومات لمخاطر الأمن السيبراني، أن مستوى الوعي العام ليس منخفضًا حسب مقياس الدراسة، حيث بلغ المتوسط الحسابي العام لجميع فقرات قياس مستوى الوعي لمفردات البحث(2.73)، وبإنحراف معياري قدره (0.60)، وهذا ما يفسر وجود وعي نسبي لدى عينة الدراسة، ما يعني عدم تحقق الفرضية التي إفترضت إنخفاض الوعي.

ويرجع ذلك أن لدى الأخصائيين وعيًا قانونيًا مقبولًا بحوكمة المعلومات، يُرجح إرتباطه بالتكوين أو بالتوجيهات الإدارية داخل الجامعات. كما أبانت النتائج عن إدراك جيد لأهمية تأمين البيانات، خصوصًا في جانب التحكم في الوصول، بما يعكس فهمًا واضحًا لأحد مرتكزات الحماية الأساسية، غير أن مستوى الوعي بمخاطر الأمن السيبراني ظل في مجمله متوسطًا بمتوسط حسابي (0.60)، كما برزت مؤشرات مقلقة تتمثل في ضعف فهم المسؤوليات الفردية المتعلقة بحماية المعلومات الحساسة، ووجود شكوك حول فعالية السياسات المعتمدة، إضافة إلى تفاوت جهود التدريب وميولها للطابع النظري أكثر من التطبيقي.

تشير دلالة هذه النتائج إلى أن المشكلة ليست في غياب الوعي تمامًا، بل في "فجوة إنتقال" من الوعي إلى التطبيق المنضبط. فوجود وعي قانوني مقبول لا يكفي وحده ما لم يُترجم إلى إجراءات تشغيلية واضحة ومسؤوليات محددة وآليات متابعة ومراجعة.

كما أن وجود وعي جيد بالتحكم في الوصول لا يضمن الحماية إذا لم تُدعّم هذه القناعة بضوابط مؤسسية مثل: إدارة الهوية والصلاحيات، مراجعات دورية للحسابات، وتوثيق واضح للصلاحيات، وإجراءات دقيقة لإدارة كلمات المرور والمصادقة. كذلك فإن ضعف فهم المسؤوليات الفردية يكشف عن خلل في جانب "ثقافة الأمن" داخل المؤسسة، وهو خلل يرفع المخاطر حتى لو توفرت بعض التقنيات؛ لأن العامل البشري يبقى المدخل الأكثر شيوعًا للاختراقات عبر أخطاء بسيطة مثل مشاركة كلمات المرور، أو الاستجابة للتصيد، أو استخدام أجهزة غير مؤمّنة على الشبكة.

- **تفسير نتائج إختبار الفرضية الثانية**

"مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات المركزية لجامعات الشرق الجزائري متوسط".

أكدت نتائج الدراسة أن مستوى تطبيق مبادئ حوكمة المعلومات بالمكتبات محل الدراسة متوسط، حسب مقياس الدراسة حيث بلغ المتوسط الحسابي لجميع مجالات المحور الأول (2.65)، وإنحراف معياري (0.50)،

نلاحظ وجود تباين في مستوى حوكمة المعلومات،حيث نجد بعد "الإمتثال"في المرتبة الأولى بمتوسط حسابي نسبي بلغ (2.71)، حيث سجلت بعض فقراته تبنٍي منخفضة، مثل ضعف تنفيذ إجراءات الكشف عن المخالفات أو المراجعة الدورية للإمتثال. وعموما سجل بعد الإمتثال درجة متوسطة.كما نلاحظ أن بعد "الإستبعاد"في المرتبة الثانية بمتوسط حسابي (2.68)، يعكس إفتقار أخصائي المعلوماتإلى بعض جوانب الموثوقية والإنتظام، خاصة في ما يتعلق بالتوثيق والتدريب المستمر.

أما بعد "المسؤولية"فقد جاء في المرتبة الثالثة بمتوسط حسابي نسبي (2.62)، تم تسجيل ضعف واضح في التدريب وتعزيز ثقافة المسؤولية الفردية عند أخصائي المعلومات. في حين أظهرت النتائج أن بعد "الحفظ" أضعف مستوى بمتوسط حسابي (2.60)، وبالنظر إلى أهميته في ضمان حماية وسلامة البيانات وهذا يدل على وجود تهديدات وأخطار محتملة.

وفي ضوء ما سبق، أظهرت نتائج الدراسة إلى وجود تباين في تطبيق أبعاد حوكمة المعلومات في المكتبات المركزية لجامعات الشرق الجزائري، أظهرت صحة الفرضية الرئيسة وفق مؤشرات أبعادها، إذ جاءت النتيجة العامة عند مستوى متوسط.

على مستوى الأبعاد الفرعية، ظهر أن تطبيق المسؤولية والامتثال والحفظ والاستبعاد جميعها في مستوى متوسط. تُظهر دلالة هذا النمط أن الحوكمة في المكتبات محل الدراسة موجودة "كفكرة وتوجه"، لكنها لا تزال بحاجة إلى توحيدها في نظام عمل مؤسسي متكامل يقوم على: سياسات مكتوبة وموحّدة، أدوار ومسؤوليات محددة، إجراءات تشغيل معيارية، وثائق وسجلات متابعة، وآليات قياس وتدقيق وتحسين مستمر.

كما يشير المستوى المتوسط للأبعاد الأربعة إلى احتمال وجود تطبيق غير متوازن؛ أي أن بعض المكتبات قد تُحسن جانبًا (مثلاً الوصول)، لكنها تضعف في جوانب أخرى أكثر حساسية مثل إدارة دورة حياة البيانات أو الاستبعاد الآمن والتوثيق المرتبط به.

- **تفسير نتائج إختبار الفرضية الثالثة:**

"مستوى مخاطر الأمن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي".

أكدت نتائج إختبار الفرضية وفق أبعاد الأمن السيبراني لأخصائي المعلومات أن مستوى مخاطر الأمن السيبراني في المكتبات الجامعية محل الدراسة أخذ درجة متوسطة حسب مقياس الدراسة، بمتوسط حسابي يبلغ (2.84).

وأظهرت ترتيب أبعاد قياس مستوى مخاطر الأمن السيبراني سجل درجة متوسطة مع تصدر بعد المخاطر العامة قائمة المخاطر المدركة من قبل أخصائي المعلومات، وهذا يرجع إلى درايتهم بالتهديدات والمخاطر التي تهدد المكتبات الجامعية ونظمها في شبكة الانترنت، وخبرتهم في المجال، ويليها بعد التوافر والسلامة والسرية على التوالي. هه المعطيات تثبت عدم صحة الفرضية الرئيسة الثالثة.

في حين أظهرت نتائج إختبار أن المخاطر جاءت عند مستوى عالٍ في جميع الأبعاد: السرية، السلامة/النزاهة، التوافر، والمخاطر العامة، وهو ما يؤكد فرضية الدراسة الثالثة. وتكمن دلالة هذا الإرتفاع في أن البيئة الرقمية للمكتبات محل الدراسة تواجه تهديدات فعلية ومتعددة،وأن أنماط الحماية الحالية (التي تقف عند مستوى متوسط في الحوكمة) ليست كافية لتخفيض المخاطر إلى مستوى مقبول. كما تعني هذه النتائج أن أي خلل في الضبط التنظيمي (سياسات، أدوار، تواصل داخلي) أو الخلل في تدريب الموظفين أو توثيق الإجراءات، قد يتحول بسرعة إلى ثغرة تمس سرية بيانات المستفيدين، أو سلامة المحتوى الرقمي، أو استمرارية الخدمات الأكاديمية (قواعد البيانات، المستودعات، الإعارة الإلكترونية، الفهرسة).

- **تفسير نتائج إختبار الفرضية الرابعة**

"أثر تطبيق حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات المركزية لجامعات الشرق الجزائري عالي"

أظهرت نتائج معطيات المحور الرابع المتعلق بأثر تطبيق حوكمة المعلومات على مخاطر الأمن السيبراني، تحقق الفرضية الرابعة، حيث ظهر وجود أثر مرتفع لأبعاد حوكمة المعلومات على مخاطر الأمن السيبراني، وشمل ذلك أثر السياسات الداخلية ومسؤولية الأفراد، وأثر التشريعات والمعايير العالمية، وأثر كفاءة نظام دورة حياة البيانات، وأثر فعالية وأمان عمليات الاستبعاد.

تعد هذه النتيجة جوهرية لأنها تقدم تفسيرًا عمليًا لما سبق، والمتمثل في النقاط التالية:

- إرتفاع المخاطر يقترن بإنخفاض/متوسطية تطبيق الحوكمة.
- تحسن الحوكمة يؤدي إلى خفض المخاطر. ودلالتها الإدارية واضحة: معالجة المخاطر السيبرانية في المكتبات الجامعية
- لا ينبغي أن تُختزل في شراء أدوات أو برمجيات فقط، بل يجب أن تنطلق من بناء منظومة حوكمة تُحوّل الأمن إلى ''سياسة مؤسسية'' لها مسؤوليات وميزانية وخطط قياس وتقييم، بما يضمن الاستدامة والفعالية.

- **تفسير نتائج إختبار الفرضية الخامسة**

"لا توجد فروق ذات دلالة احصائية في مستوى مخاطر الامن السيبراني تعزى السوسيوديمغرافية لأخصائي المعلومات بالمكتبات محل الدراسة"

بيّنت نتائج إختبار الفروق عدم وجود فروق دالة إحصائيًا تعزى لمتغير الجنس أو الخبرة المهنية، في حين ظهرت فروق دالة تعزى لمتغير الرتبة الوظيفية، كما ظهرت فروق دالة حسب جامعة العمل. وتكمن دلالة هذه النتائج في أن إدراك المخاطر لا يرتبط بخصائص شخصية بقدر ما يرتبط بموقع الفرد داخل الهيكل الوظيفي وبالسياق المؤسسي الذي تعمل فيه المكتبة.

فإختلاف الرتب يعني إختلاف مستوى الإطلاع على السياسات والقرارات والتهديدات، وإختلاف الجامعات يشير إلى تباين في البنية التحتية التقنية، ومستوى الدعم الإداري، وجودة التواصل الداخلي، ومدى الإستثمار في الأمن والتدريب. وهذا يقود إلى دلالة تطبيقية مهمة: التوصيات يجب أن تجمع بين "حلول موحّدة "على مستوى حوكمة المكتبات الجامعية عمومًا، و"حلول موجهة" بحسب الرتب (تحديد أدوار ومسؤوليات ومسارات تدريب مختلفة) وبحسب خصوصية كل جامعة (خطط تحسين تدريجية وفق فجواتها الفعلية).

كما أظهرت نتائج الدراسة الميدانية، على مستوى خصائص العينة مجموعة من النتائج وهي كالآتي:

- أن أخصائيّي المعلومات بالمكتبات الجامعية في الشرق الجزائري يغلب عليهم مستوى الليسانس والماستر، في حين تمثل الدكتوراه نسبة محدودة مقارنة بباقي المستويات العلمية.
- وجود تنوع في الرتب الوظيفية داخل المكتبات محل الدراسة، مقابل محدودية الرتب العليا في الهرم الإداري.
- أن أخصائي المعلومات بالمكتبات المركزية وفق مؤشر الخبرة المهنية يتسم بطابع "خبير"، إذ تشكل فئة الموظفين ذوي الخبرة المتوسطة إلى الطويلة النسبة الأكبر، تكمن دلالة هذه النتائج في أن المورد البشري في المكتبات الجامعية يمتلك قاعدة معرفية وخبرة عملية تسمح بفهم متطلبات الحوكمة والأمن السيبراني.
- محدودية الرتب العليا قد تؤثر في سرعة إتخاذ القرار وتفعيل المساءلة والرقابة العليا وتخصيص الموارد اللازمة لتطبيق الحوكمة على نحو أكثر نضجًا.
- أن الخبرة لا تعني بالضرورة إمتلاك مهارات أمنية تقنية محدثةما يستدعي إسناد الخبرة إلى تدريب نوعي ومستمر يواكب تطور التهديدات الرقمية.

إستنادا لما سبق، تتمثل الصورة العامة التي ترسمها نتائج الدراسة في مايلي:

- وجود وعي مفاهيمي وقانوني مقبول نسبيًا يقابله تطبيق متوسط لمبادئ الحوكمة، وفي المقابل مستوى مرتفع لمخاطر الأمن السيبراني. وهو ما يدل على فجوة تنفيذية تتطلب تحويل الحوكمة إلى ممارسات تشغيلية قابلة للقياس والتدقيق والتحسين.
- إعطاء أولوية لتوضيح المسؤوليات الفردية، وإعادة تفعيل الإتصال الداخلي حول السياسات والمعايير.
- تعزيز التدريب التطبيقي، وتوحيد إجراءات إدارة البيانات عبر دورة حياتها.
- التشدد في بعد الإستبعاد الآمن والتوثيق المصاحب له.
- تشكّل هذه الدلالات قاعدة مباشرة لصياغة التوصيات، بحيث تُوجَّه نحو رفع مستوى الحوكمة (تنظيميًا وبشريًا وتقنيًا) بوصفه المدخل الأكثر تأثيرًا في خفض المخاطر السيبرانية داخل المكتبات الجامعية.

7.6 مقارنة نتائج الدراسة بنتائج الدراسات السابقة

تُظهر نتائج الدراسة الحالية أن مستوى وعي أخصائيّي المعلومات بحوكمة المعلومات المرتبطة بمخاطر الأمن السيبراني متوسط، وأن مستوى تطبيق مبادئ حوكمة المعلومات داخل المكتبات الجامعية محل الدراسة متوسط عمومًا، مع تفاوت واضح بين الأبعاد؛ إذ جاء الحفظ منخفضًا مقارنة ببقية الأبعاد، في حين جاءت المسؤولية والامتثال والاستبعاد بمستوى متوسط، إلى جانب ما خلصت إليه الدراسة من أن مستوى مخاطر الأمن السيبراني مرتفع، وأن لحوكمة المعلومات أثرًا مرتفعًا في الحد من المخاطر. كما بيّنت الدراسة عدم وجود فروق دالة تعزى للخبرة المهنية، مقابل وجود فروق دالة تعزى للوظيفة في بعض الاختبارات.

1) حوكمة نظم معلومات المؤسسات: تقاطع "النضج المتوسط" مع صعوبات التطبيق

تتقاطع نتائج الدراسة الحالية خصوصًا الحكم العام بأن تطبيق مبادئ الحوكمة متوسط مع وجود أبعاد ضعيفة (الحفظ)، مع ما توصلت إليه دراسة مسوس كمال (2018) التي أشارت إلى أن واقع نظم المعلومات الحديثة وإدارتها في مؤسسات التعليم العالي لا يساعد بما يكفي على التوجه نحو حوكمة نظم المعلومات، وأن التوجه نحو الحوكمة يتطلب مقومات تنظيمية وممارسات فعلية تتجاوز مجرد وجود أنشطة متفرقة.

وجه الاتفاق هنا يتمثل في أن كلا الدراستين لا يقدمان صورة "حوكمة مكتملة"، بل يبرزان فجوة بين التوجه والوجود الشكلي وبين الممارسة المؤسسية المتكاملة. غير أن الدراسة الحالية تُفصّل هذه الفجوة على مستوى أبعاد محددة (الحفظ، الاستبعاد، الامتثال...) داخل بيئة المكتبات الجامعية نفسها، وهو تفصيل لم يكن محور دراسة مسوس التي انصبت على نظم المعلومات في مؤسسات التعليم العالي على نحو أوسع.

2) الحوكمة كمدخل للجودة الشاملة: اتفاق جزئي وتحول في زاوية النظر

تتوافق نتائج الدراسة الحالية، ولا سيما ما خلصت إليه من أن لحوكمة المعلومات أثرًا مرتفعًا في الحد من المخاطر، مع ما عرضته عن دراسة زيادي كريمة (2023) التي انتهت إلى أن تطبيقات الحوكمة تسهم بفاعلية في تحقيق الجودة الشاملة عبر تعزيز الشفافية والمساءلة والتعاون، وترتبط بالتخطيط والتنظيم والرقابة وتقييم الأداء.

وجه الاتفاق يتمثل في الإقرار بدور الحوكمة كآلية تنظيمية تُحسن الأداء المؤسسي وتقلل الهشاشة. لكن الاختلاف أن الدراسة الحالية تُسقط هذا الدور مباشرة على إدارة المخاطر السيبرانية داخل المكتبات، وتُظهر أن أثر الحوكمة لا يقتصر على الجودة الإدارية العامة، بل يمتد إلى ضبط جوانب حساسة في LIS مثل حماية المعطيات الشخصية للمستفيدين، وسلامة البيانات الوصفية الناتجة عن الفهرسة والتصنيف، واستمرارية الإتاحة الرقمية. وبذلك تتحول الحوكمة هنا من "رافعة جودة" إلى "رافعة أمن معلومات" داخل مؤسسة معلوماتية.

3) التدريب ونقل المعرفة: اتساق مع الأدبيات وتفسير الفجوات

تنسجم نتائج الدراسة الحالية التي تشير إلى أن الوعي العام متوسط مع وجود جوانب أضعف في الممارسة التقنية/الإجرائية (خصوصًا الحفظ وتوثيق الاستبعاد) مع ما ورد في دراسة Nicolas-Rocca (2019) حول أن تعليم الأمن السيبراني ونقل المعرفة يمكن أن يعززا استخدام المعرفة، ويؤثران في الموظفين عبر المناقشات المتعلقة بالمساءلة والمسؤولية وزيادة الوعي بحماية معلومات المستفيدين.

وجه الاتفاق واضح في أن التوعية/التدريب يمثلان قناة مركزية لرفع الوعي المهني بالأمن داخل المكتبات. غير أن الدراسة الحالية تضيف، من واقع نتائجها، أن الوعي وحده لا يكفي؛ إذ ما يزال "الترجمة التطبيقية" متعثرة في عمليات ترتبط بدورة حياة المعلومات، مثل الحفظ طويل المدى، وسياسات الاحتفاظ، وتوثيق إجراءات المصير

النهائي للبيانات. وهذا يُفسَّر ضمن منطق Nicolas-Rocca) بأن نقل المعرفة قد يرفع مستوى الإدراك، لكنه يحتاج إلى بيئة تنظيمية وإجرائية تحوّله إلى إجراءات عمل (سياسات مكتوبة، تدريب عملي، متابعة).

4) مرجعية الحوكمة وأطرها: اتساق مع الدعوة إلى الأطر المعيارية

ترتبط نتائج الدراسة الحالية خصوصًا تفاوت أبعاد الحوكمة وضعف "الحفظ" بما عرضته عن دراسة Ahlan وآخرين (2014) التي اقترحت مرجعية (COBIT) لدعم حوكمة نظم المعلومات مستقبلًا، بعد الاعتماد على المقابلات وجمع الوثائق.

وجه الاتفاق هنا أن كلا الدراستين يلمّح إلى أن الحوكمة تحتاج إلى إطار مرجعي منظم يضمن التكامل والاتساق، بدل بقاء الممارسات متفرقة. وتُقدّم الدراسة الحالية دليلًا تطبيقيًا على الحاجة لمثل هذا الإطار عبر إبراز بُعد "الحفظ" كبؤرة ضعف؛ وهو بُعد غالبًا ما يتحسن عندما تُدار الحوكمة وفق أطر واضحة تُلزم بوجود سياسات احتفاظ، ومسؤوليات، وتدقيق، وتوثيق.

5) نضج الحوكمة في الإدارات العامة: توافق على مستوى "الإدراك" مع تباين في السياق

يتقاطع الحكم العام في الدراسة الحالية بأن مستوى تطبيق الحوكمة متوسط مع دراسة (ANDERFUHREN & ROMAGNOLI,2018) حول "نضج حوكمة المعلومات في الإدارات العامة الأوروبية: تصور الحوكمة".

وجه التقاطع هنا مفهومي: كلا السياقين يشتغل على مستوى النضج، التصور، التطبيق. غير أن الدراسة الحالية تنتمي إلى بيئة مكتبية جامعية في الجزائر، ما يجعل تفسير "المتوسط" مختلفًا من حيث البنية التحتية الرقمية، والموارد، والتدريب، وآليات التوثيق. لذا فإن التوافق هنا هو توافق في "منطق القياس"(نضج،تصور،تطبيق) أكثر منه تطابقًا في النتائج التفصيلية، لأن الدراسة الأجنبية تختلف موضوعيًا وسياقيًا.

6) الفروق حسب الخبرة والوظيفة: إضافة نوعية للدراسة الحالية مقارنة بما عرضته من أدبيات

فيما لا تُظهر الدراسات السابقة تركيزًا صريحًا على اختبار الفروق تبعًا للخبرة المهنية والوظيفة داخل المكتبات، تقدّم الدراسة الحالية إضافة تفسيرية مهمة: عدم وجود فروق حسب الخبرة المهنية يقابله وجود فروق حسب الوظيفة في بعض النتائج.

هذه النتيجة يمكن قراءتها مهنيًا داخل LIS على أن إدراك المخاطر لا يتحدد بالخبرة الزمنية وحدها، بل يتأثر بـ موقع الفرد في سير العمل المكتبي وطبيعة التعامل مع البيانات مثل: موظفو الإعارة وبيانات المستفيدين، وموظفو

الفهرسة والتصنيف والبيانات الوصفية، والإدارة والإشراف. وهذا يُسهم في تطوير فهم أكثر دقة لتوزيع المخاطر والمسؤوليات داخل المكتبة الجامعية.

- **خلاصة المقارنة**

تُظهر المقارنة أن الدراسة الحالية تتفق مع الدراسات المعتمدة في نقطتين رئيستين:

1. الحوكمة لا تزال تواجه تحديات تطبيقية، وأن وجود سياسات أو توجهات عامة لا يعني اكتمال النضج المؤسسي (مسوس، 2018).

2. أن التدريب ونقل المعرفة ركيزة مركزية لرفع الوعي وحماية معلومات المستفيد (Nicolas-Rocca، 2019)،

3. تتقاطع مع الدراسات التي تنظر للحوكمة كرافعة لتحسين الأداء المؤسسي (زيادي، 2023) وكحاجة إلى أطر مرجعية داعمة (Ahlan وآخرون، 2014). وفي الوقت نفسه، تتميز الدراسة الحالية بإضافة واضحة تتمثل في تفكيك الحوكمة إلى أبعاد داخل المكتبة الجامعية، وإبراز "الحفظ" كبؤرة ضعف، وربط ذلك بمستوى مخاطر مرتفع، ثم اختبار الفروق حسب المتغيرات (الخبرة والوظيفة) بما يمنح نتائجها قيمة تفسيرية مباشرة للاختصاص.

8.6 مقترحات وتوصيات الدراسة

إستنادًا إلى النتائج التي توصلت إليها الدراسة الميدانية، والتي بيّنت أن مستوى تطبيق حوكمة المعلومات بالمكتبات الجامعية محل الدراسة جاء في حدود المستوى المتوسط مقابل إرتفاع مستوى مخاطر الأمن السيبراني، ومع ثبوت الأثر المرتفع لأبعاد الحوكمة على خفض المخاطر، توصي الدراسة بما يلي:

أ. توصيات على المدى القريب (0–3 أشهر)

1. إعداد سياسة مكتوبة ومختصرة لأمن المعلومات داخل المكتبة تتضمن: تصنيف البيانات، ضوابط الوصول، إجراءات النسخ الاحتياطي، وآليات الإبلاغ عن الحوادث، مع تعميمها وتوضيحها للعاملين.

2. تسمية منسق/مسؤول لحوكمة المعلومات والأمن السيبراني داخل المكتبة (ولو بالتكليف) مع تحديد مهامه وصلاحياته رسميًا.

3. إجراء مراجعة عاجلة للصلاحيات الممنوحة للحسابات الحساسة والحسابات الإدارية واعتماد مبدأ "أقل صلاحية" في منح الأذونات.

4.فرض المصادقة متعددة العوامل (MFA) للحسابات الإدارية وحسابات الوصول عن بعد، بوصفها إجراءً وقائيًا عاجلًا للحد من اختراق الحسابات.

5.توحيد تفعيل سجلات التدقيق (Logs) للأنظمة الحيوية وربطها بمراجعة دورية مختصرة لرصد السلوك غير الطبيعي ومحاولات التسلل.

6.إعتماد سياسة دورية للتحديثات الأمنية (Patch Management) وتوثيق تنفيذها لضمان تقليل الثغرات القابلة للاستغلال.

7.إقرار حد أدنى لإجراءات النسخ الاحتياطي مع اختبار استعادة دوري لضمان استمرارية الخدمات وتقليل أثر الحوادث.

8.تنفيذ برنامج توعوي سريع ومباشر للعاملين حول: التصيد الإلكتروني، كلمات المرور، مشاركة الحسابات، الأجهزة الشخصية، وإجراءات الإبلاغ عن الحوادث.

9.إعتماد "تعهد استخدام آمن" يوضح المسؤوليات الفردية وحدود الصلاحيات بما يعزز ثقافة الالتزام ويقلل المخاطر الناتجة عن السلوكيات غير الآمنة.

10.تفعيل قناة اتصال داخلية ثابتة داخل المكتبة لتعميم المستجدات الأمنية والتعليمات التنظيمية، بما يعالج ضعف التواصل الداخلي ويحد من الشكوك حول فعالية السياسات.

ب.توصيات على المدى المتوسط (3–12 شهرًا)

11.تشكيل لجنة/فريق حوكمة معلومات وأمن سيبراني داخل المكتبة تضم ممثلين عن المكتبة وتقنية المعلومات، وتتولى المتابعة الدورية والتوثيق.

12.إنشاء سجل مخاطر (Risk Register) خاص بالمكتبة يُحدّث بصورة دورية ويُستخدم في ترتيب الأولويات وتوجيه القرارات.

13.إعداد إجراءات تشغيل معيارية (SOPs) لعمليات أساسية، أهمها: إدارة الحسابات والصلاحيات، إدارة التغيير، النسخ الاحتياطي، إدارة الحوادث، وحماية البيانات الحساسة.

14.تعزيز أنظمة إدارة الهوية والصلاحيات (IAM) و/أو الدخول الموحد (SSO) بما يضمن ضبط الوصول وفق الأدوار وتقليل المخاطر المرتبطة بتعدد الحسابات وضعف التحكم فيها.

15. تحسين الضوابط الشبكية الأساسية (مثل تقسيم الشبكة للخوادم الحساسة وضبط الجدار الناري وفق سياسة مكتوبة).

16. إعتماد أو تطوير أنظمة كشف/منع التسلل (IDS/IPS) وربطها بإجراءات إنذار واستجابة محددة وواضحة.

17. إعداد خطة رسمية للاستجابة للحوادث تتضمن السيناريوهات المحتملة، ومسارات التصعيد، وآليات العزل والتعافي، مع تنظيم تمارين محاكاة دورية.

18. تصميم برنامج تدريب تطبيقي دوري للعاملين (محاكاة تصيد، إدارة كلمات المرور، إجراءات الإبلاغ)، مع اعتماد "سفراء أمن" داخل المكتبة لتسهيل المتابعة والتواصل.

19. توحيد دليل إجرائي على مستوى الجامعة (أو الوصاية) لحوكمة المعلومات بالمكتبات الجامعية يتضمن قوالب سياسات ونماذج توثيق وإجراءات معيارية.

20. تخصيص بند ميزانية سنوي للأمن السيبراني في المكتبات وربطه بمؤشرات قياس واضحة لضمان الاستدامة وتقليل الفجوة بين المكتبات.

ج. توصيات على المدى الطويل (سنة–3 سنوات)

21. بناء منظومة قياس وتحسين مستمر عبر مؤشرات أداء ومخاطر (KPIs/KRIs) مثل: نسبة تفعيل MFA، زمن الاستجابة للحوادث، نسبة تحديث الأنظمة، نتائج اختبارات الاستعادة، وعدد الحوادث المرصودة.

22. تفعيل إدارة دورة حياة البيانات بصورة رسمية ومتكاملة (تصنيف، احتفاظ، أرشفة، استبعاد) وربطها بالتوثيق والمساءلة، بما يقلل نطاق الضرر ويرفع الامتثال.

23. التدرج نحو مواءمة سياسات وإجراءات المكتبات مع الأطر والمعايير الدولية (مثل ISO/IEC 27001 أو NIST CSF) وفق خطة مرحلية قابلة للتنفيذ.

24. إنشاء أو تفعيل نقطة تنسيق جامعية للاستجابة للحوادث أو فريق متخصص يقدم الدعم للمكتبات التابعة (Incident Response/SOC) مصغر.

25.تعزيز التعاون بين الجامعات لتبادل الخبرات والإنذارات وأفضل الممارسات، بما يرفع الجاهزية ويقلل من تكرار الأخطاء.

26.تعزيز حوكمة الموردين والخدمات السحابية عبر عقود تتضمن متطلبات أمنية واضحة (التشفير، حماية البيانات، الإبلاغ عن الحوادث، وحقوق التدقيق)، خصوصًا مع تنامي الاعتماد على المحتوى المرخّص والخدمات الرقمية الخارجية.

27.إدماج الأمن السيبراني وحوكمة المعلومات ضمن خطة تطوير الموارد البشرية (تكوين سنوي إلزامي + مسارات تخصصية) لضمان استمرارية بناء القدرات ومواكبة التهديدات المتغيرة.

تؤكد الدراسة أن خفض مخاطر الأمن السيبراني في المكتبات الجامعية يتطلب مقاربة شاملة لا تقتصر على الأدوات التقنية، بل تقوم على منظومة حوكمة معلومات متكاملة تتضمن سياسات واضحة، ومسؤوليات محددة، وإجراءات معيارية موثقة، وآليات قياس ومراجعة وتكوين مستمر، بما يضمن حماية الأصول المعلوماتية واستمرارية الخدمات الرقمية وتعزيز الثقة في البيئة الأكاديمية.

خاتمة

خاتمة

إن التحول الرقمي الذي تشهده المكتبات الجامعية الجزائرية، وما ترتب عنه من توسّع في الخدمات الإلكترونية والأنظمة الشبكية وقواعد البيانات الأكاديمية، قد جعل بيئة المكتبات أكثر إتباطًا بمنظومة الأمن السيبراني وبمستوى نضج الحوكمة داخل المؤسسة. وبناءً على ذلك، جاءت هذه الدراسة لتتناول إشكالية جوهرية تتمثل في : أثر حوكمة المعلومات على مخاطر الأمن السيبراني في المكتبات الجامعية، مع التركيز على المكتبات الجامعية بالشرق الجزائري بوصفها مجالًا ميدانيًا يعكس بصورة كبيرة واقعًا قابلًا للتمثيل ضمن السياق الوطني العام.

لقد أظهرت نتائج الدراسة الميدانية أن مستوى وعي أخصائيي المعلومات بمخاطر الأمن السيبراني متوسط، وأن الوعي القانوني بحوكمة المعلومات مقبول نسبيًا، غير أن ذلك لم ينعكس دائمًا على مستوى التطبيق العملي؛ إذ تبيّن وجودفجوة بين الوعي والممارسة، ووجود تفاوت في التدريب والتكوين، إلى جانب ضعف في فهم المسؤوليات الفردية في حماية المعلومات الحساسة، ووجود شكوك حول فعالية السياسات المعتمدة بسبب قصور التواصل الداخلي. وتُعد هذه المؤشراتمن منظور الحوكمةمفسِّرة لإرتفاع المخاطر، لأن المخاطر السيبرانية لا تتولد فقط من الثغرات التقنية، بل كذلك من قصور السياسات، وعدم وضوح الأدوار، وضعف ثقافة الامتثال، وتشتت الجهود بين الوحدات الإدارية، وعدم انتظام برامج التدريب والمتابعة.

وعليه، فإن معالجة مخاطر الأمن السيبراني في المكتبات الجامعية لا يمكن أن تتحقق عبر أدوات تقنية منفصلة فحسب، بل تتطلب مشروعًا مؤسسيًا متكاملًا يدمج بين الحوكمة والتنظيم والامتثال والتكوين التقني والسلوك المهني. ومن ثم، فإن المخرجات التطبيقية لهذه الدراسة يمكن تلخيصها في خمسة مشاريع وركائز تنفيذية تُعدّ أساسًا لتفعيل توصيات الدراسة وتحويلها إلى خطة مؤسسية قابلة للقياس والمتابعة:

المشروع الأول: مشروع بناء القدرات والتكوين التطبيقي

يُعدّ هذا المشروع حجر الأساس في تقليل المخاطر السيبرانية، بالنظر إلى أن نتائج الدراسة أظهرت مستوى وعي متوسطًا ووجود تباين في التكوين. ويقتضي ذلك الانتقال من التكوين النظري إلى تدريب تطبيقي منتظم يشمل: التصيد الإلكتروني، إدارة كلمات المرور، قواعد الإستخدام الآمن، الإبلاغ عن الحوادث، وضبط السلوكيات عالية الخطورة (مثل مشاركة كلمات المرور أو ضعف التحقق). كما يستهدف المشروع بناء "ثقافة امتثال" تجعل العاملين جزءًا من منظومة الحماية لا نقطة ضعف فيها، مع قياس أثر التدريب بمؤشرات واضحة (اختبار قبلي/بعدي، محاكاة تصيد، نسبة الالتزام بالضوابط).

المشروع الثاني: مشروع تهيئة البيئة التنظيمية والحوكمة داخل المكتبات

أكدت الدراسة أن جانبًا معتبرًا من المخاطر يرتبط بعوامل تنظيمية (ضعف المسؤولية الفردية، ضعف التواصل الداخلي، شكوك حول السياسات). وعليه، يهدف هذا المشروع إلى توفير بيئة قابلة لتطبيق الحوكمة عبر:

- إقرار سياسات مكتوبة لأمن المعلومات وحوكمة البيانات وتعميمها وتوضيحها.
- تحديد الأدوار والمسؤوليات ومسارات المساءلة رسميًا داخل المكتبة.
- تفعيل قنوات اتصال داخلية لإشعار العاملين بالتحديثات والمعايير والإجراءات.
- اعتماد سجل مخاطر وتحديد أولويات المعالجة.
- دمج الحوكمة ضمن الإدارة الاستراتيجية للمكتبة وربطها بأهداف الجامعة.

ويُعد هذا المشروع شرطًا سابقًا لنجاح الضوابط التقنية، لأن التقنية دون تنظيم وسياسة ومسؤولية تبقى محدودة الأثر.

المشروع الثالث: مشروع مواءمة الأطر والمعايير وتحويلها إلى إجراءات تشغيلية

لضمان أن توصيات الدراسة لا تبقى في حدود العموميات، يقترح هذا المشروع إعتماد مرجعيات معيارية تُحوَّل إلى إجراءات قابلة للتنفيذ، وذلك وفق بناء طبقي:

- حوكمة القيادة ISO/IEC 38500 مع COBIT 2019.
- نظام إدارة أمن المعلومات ISO/IEC 27001/27002.
- إدارة المخاطر والاستجابة للحوادث ISO/IEC 27005 و ISO/IEC 27035.
- إدارة الخدمات واستمرارية الأعمال ITIL 4 و ISO 22301.
- حماية البيانات،الخصوصية عند الاقتضاء ISO/IEC 27701 :

وتتمثل القيمة المضافة لهذا المشروع في أنه يجعل التطبيق قابلاً للتدقيق والقياس والتحسين المستمر، بدل أن يكون جهودًا متفرقة غير موحدة بين المكتبات.

المشروع الرابع: مشروع الضوابط التقنية ورفع الجاهزية التشغيلية

وهو المشروع الذي يترجم الحوكمة إلى "واقع تقني" يقلل المخاطر بصورة مباشرة، ويشمل:

- إدارة الهوية والصلاحيات IAM وتفعيل MFA للحسابات الحساسة.
- تشفير البيانات الحساسة أثناء النقل والتخزين عند الاقتضاء.

- تفعيل سجلات التدقيق وربطها بالمتابعة والتحليل.
- اعتماد IDS/IPS أو بدائل مناسبة لرصد الأنشطة المشبوهة.
- النسخ الاحتياطي وفق سياسة موحدة مع اختبارات استرجاع دورية.
- خطةاستجابة للحوادث وتمارين محاكاة دورية.

وتمثل هذه الضوابط الحد الأدنى العملي الذي يحقق خفضًا ملموسًا في المخاطر، بشرط أن تُدار ضمن المشروع الثاني والثالث (السياسات، المعايير،المسؤوليات).

المشروع الخامس: مشروع الحوكمة المؤسسية على مستوى الجامعة والتنسيق البيني

لأن المكتبات الجامعية تعمل ضمن منظومة جامعية أوسع، فإن نجاح خفض المخاطر يتطلب مستوى من التنسيق المؤسسي يتجاوز حدود المكتبة الواحدة، ويشمل:

- توحيد حد أدنى وطني، جامعي للسياسات والإجراءات.
- توفير دعم مركزي (لجنة، فريق استجابة، مرجعية تقنية) يخدم المكتبات التابعة.
- إدراج الأمن السيبراني وحوكمة المعلومات ضمن التخطيط الجامعي والتمويل.
- تعزيز التعاون بين الجامعات لتبادل الخبرات وأفضل الممارسات والتحذيرات.

وتكمن أهمية هذا المشروع في تقليل التفاوت بين الجامعات وتقليص فجوة الموارد والجاهزية.

توصي الدراسة بتوجيه البحوث المستقبلية نحو:

- دراسات طولية تقيس أثر تطبيق مشاريع الحوكمة والتدريب على مستوى المخاطر قبل/بعد.
- دمج أدوات قياس موضوعيةLogs) ، مؤشرات الحوادث، تدقيق الامتثال، زمن الاستجابة.(
- بناء نموذج نضج (Maturity Model) خاص بالمكتبات الجامعية يربط بين مستويات الحوكمة ومستويات المخاطر ومؤشرات.KPIs/KRIs
- دراسات مقارنة بين جامعات مختلفة وفق الموارد والتقنيات والبنية التنظيمية.
- بحث إشكالية التوازن بين الإتاحة الأكاديمية ومتطلبات الأمن السيبراني، خاصة مع توسع الخدمات السحابية والوصول عن بعد.

وبناءً على ما تقدم يؤكد الباحث أن رفع مستوى حوكمة المعلومات يمثل مدخلًا حاسمًا لخفض مخاطر الأمن السيبراني في المكتبات الجامعية، وأن نجاح هذا المدخل يتطلب تنفيذًا مرحليًا عبر مشاريع متكاملة تشمل: بناء القدرات، تهيئة البيئة التنظيمية، مواءمة المعايير، تفعيل الضوابط التقنية، وتطوير التنسيق المؤسسي على

خاتمة

مستوى الجامعة. وبذلك يمكن للمكتبات الجامعية تعزيز استمرارية خدماتها الرقمية وحماية بيانات المستفيدين وترسيخ الثقة في البيئة الأكاديمية.

قائمة

بيبليوغرافية

قـائمة بيبليوغرافية

❖ **قواميس ومعاجم.**

1. قاموساكسفورد.معجم اكسفورد. بريطانيا: جامعة أكسفورد، 2019.

❖ **كتب**

2. بن خضير، أحمد بن عبد الله. **حوكمة المعلومات مبادئ، استراتيجيات وأفضل الممارسات**. دار جامعة الملك سعود للنشر. الرياض،2024
3. دشلي،كمال .**منهجية البحث العلمي** .حماة: مديريةالكتبوالمطبوعاتالجامعية،2016.
4. الشامي، حسين علي. **الحوكمة والنمو الاقتصادي دراسة في دول مختارة مع إشارة خاصة للعراق**. دار غيداء. عمان. ط،01، 2019.
5. الصباغ، عماد عبد الوهاب. **علم المعلومات**. دار الثقافة والنشر والتوزيع. الأردن، 2004.
6. عبد الهادي، محمد فتحي. **المعلومات وتكنولوجيا المعلومات على أعتاب قرن جديد**. مكتبة الدار العربية للكتاب. مصر، 2000.
7. محمد مصطفي، سليمان. **حوكمة لشركات ودور أعضاء مجالس الإدارة والمديرين التنفيذيين**. دار الجامعة الإسكندرية. ط 01، 2009.
8. شوابكة، محمد أمين. **جرائم الحاسوب والأنترنيت: الجريمة المعلوماتية**. دار الثقافة والنشر والتوزيع. عمان. ط،04، 2004.
9. جيرار، بيرو. **إدارة السجلات والمحفوظات في الأمم المتحدة**. جنيف: الأمم المتحدة، 2013
10. توفيقمحمود محمد، القزاز. **الأمن السيبيراني لمصادر المعلومات**. طبعة،01. القاهرة. مؤسسة طيبة للنشر والتوزيع، 2022.
11. الطائي، محمدعبد الحسين؛ الكيلاني،محمود. **إدارة امن المعلومات**. الطبعة، 01. عمان. دار الثقافة للنشر والتوزيع، 2015.
12. الطيطي،خضر مصباح. **أساسيات امن المعلومات والحاسوب**. الطبعة،01. عمان. دار الحامد للنشر والتوزيع، 2010.
13. الحمامي، علاء حسين؛ العالي، سعد عبد العزيز. **تكنولوجيا أمنية الملومات وأنظمة الحماية**. طبعة، 01. عمان. دار وائل للنشر والتوزيع، 2007.
14. صادق، دلال؛ الفتال، حميد ناصر. **أمن المعلومات**. طبعة، 01. عمان. دار البازوزي العلمية للنشر والتوزيع، 2008.
15. الغنيمي، أشرف. **نظم الحماية من قراصنة الكمبيوتر**. طبعة، 01. القاهرة. دار الفاروق للنشر والتوزيع، 1997.
16. الحوش، محمود أبو بكر. **التقنية الحديثة في المعلومات والمكتبات**. طبعة، 01. عمان. دار الفجر للنشر والتوزيع، 2022.
17. بن عديد، سامية.**مخاطر الامن السيبراني والمعلوماتي وتطور المعرفة التقنية على برامج الحماية للأنظمة المعلوماتية**.كتاب جماعي: الأمن المعلوماتي ورقمنة قطاع التعليم: جامعة سوق أهراس، 2023.
18. بن شهيدة، محمد. **تكنولوجيا المعلومات والاتصالات في المكتبات الجامعية: الاوعية الالكترونية كحل لتحديات الحفاظ على الموارد والتحديات المستمرة**. طبعة، 01. تيارت. ألفا للوثائق للنشر والتوزيع، 2024.
19. الهمشري، عمر أحمد؛ عليان، ربحي مصطفى. **المرجع في علم المكتبات والمعلومات**. عمان:دار الشروق، 1996.

20. المدادحة، أحمد نافع. **المكتبات الجامعية ودورها في عصر المعلومات**. عمان: مكتبة المجتمع العربي، 2004.

❖ **المواثيق والأوامر**

21. الجريدة الرسمية الجزائرية. **المرسوم التنفيذي رقم 04/18 المؤرخ في 24 شعبان عام 1934 الموافق ل10 ماي سنة 2018** يتضمن القواعد العامة التعلقة بالبريد والإتصالات الرقمية، العدد 27، 2018.

22. الأمر 21- 09 المؤرخ في 27 شوال 1441 الموافق ل 08 يونيو 2021.**يتعلق بحماية المعلومات والوثائق الإدارية**. عدد45 الصادرة في 09 يونيو 2021.

❖ **رسائل وأطروحات جامعية**

23. بن عيسى، ريم. **تطبيق اليات حوكمة المؤسسات وأثرها على الأداء المالي دراسة حالة مؤسسات الجزائرية المدرجة في السوق الأوراق المالية**. مذكرة ماجستير علوم اقتصادية. كلية العلوم الاقتصادية التسيير والعلوم التجارية: تخصص اقتصاد وتسير المؤسسة. جامعة قاصدي مرباح، ورقلة، 2009.

24. بن زغده، حبيبة. **دور الحوكمة المؤسسية في تعزيز واستدامة نمو المؤسسات دراسة حالة بعض المؤسسات الاقتصادية من ولاية جيجل**. أطروحة دكتوراه. كلية العلوم الاقتصادية والتجارية وعلوم التسيير: تخصص أعمال والتنمية المستدامة. جامعة سطيف 1، 2019.

25. محي الدين، زكريا. **أليات حوكمة المؤسسة العمومية الاقتصادية: حالة المؤسسة العمومية الاقتصادية الجزائرية**. أطروحة دكتوراه، كلية العلوم الاقتصادية: تخصص المالية والمحاسبة، جامعة عبد الحميد بن باديس. الجزائر، 2020.

26. عدنان، خديجة. قيلال، حنان. **إدارة المخاطر في مؤسسات المعلومات، المكتبات العمومية في ظل جائحة كورونا دراسة ميدانية: بالمكتبة الرئيسية للمطالعة العمومية سعد دحلب_ تيارت**. مذكرة لنيل شهادة الماجستير. كلية العلوم الإنسانية والاجتماعية: علم المكتبات والتوثيق. جامعة ابن خلدون. تيارت، 2021.

27. رمزي، فهد بن عبد الرحمان مسفر. **الإدارة بالشفافية لدى مديري مكاتب التربية والتعليم بمنطقة مكة المكرمةمن وجهة نظر المديرين والمشرفين**. مذكرة ماجستير. كلية التربية: قسم الإدارة التربوية والتخطيط. جامعة أم القرى. السعودية، 2013.

28. زيادي، كريمة. **دور تطبيقات الحوكمة في تحقيق الجودة الشاملة بالمكتبات الجامعية: دراسة ميدانية بالمكتبات الجامعية لجامعات الشرق الجزائري**. أطروحة دكتوراه تخصص: إدارة وتسيير المكتبات ومراكز التوثيق. جامعة تبسة، 2024

29. العسالي، جمال. **تطبيق حوكمة الشركات في المؤسسات الصغيرة والمتوسطة كآلية لتحسين الأداء الاقتصادي في الجزائر2000-2014**. أطروحة دكتوراه. كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير: نقود مالية وبنوك. جامعة الجزائر 03. الجزائر، 2019.

30. الزاحي، سمية. **مكانة المكتبات الجامعية في سياسة التعليم العالي في الجزائر: دراسة ميدانية بجامعة منتوري قسنطينة، عنابة وسكيكدة**. أطروحة دكتوراه. قسنطينة: جامعة منتوري، 2014.

31. شتا عبد السلام علي، ابتسام. **تأمين المعلومات بمكتبات جامعة الأزهر: المكتبة المركزية نموذجا**. أطروحة لنيل شهادة الدكتوراه. كلية الدراسات الإنسانية، قسم الوثائق والمكتبات والمعلومات: تخصص الوثائق والمكتبات والمعلومات. جامعة الأزهر. القاهرة، مصر، 2023. ص 223

32. برابح إسمهان. **جاهزية المكتبات الجامعية ودورها في تطبيق اليقضة المعلوماتية لد أخصائي المعلومات: دراسة ميدانية بمؤسسات التعليم العالي والبحث العلمي ولاية عنابة**، أطروحة دكتوراه، تخصص علم المكتبات، جامعة عنابة، 2020.ص.37

33. بوربابة، صورية. **قواعد الأمن المعلوماتي**. أطروحة لنيل شهادة الدكتوراه. كلية الحقوق والعلوم الإنسانية. قسم الحقوق: تخصص قانون خاص. جامعة جيلالي اليابس. سيدي بلعباس، 2016

34. فوغالية، صربينة. **واقع انضمام المكتبة الجزائرية الى الفهرس العربي الموحد ومساهمتها من خالله في ارلساء نظام معلومات عربي: دراسة ميدانية بالمكتبة الوطنية الجزائرية ومكتبة جامعة الجزائر 3**. مذكرة ماجستير، تختصص: المعلومات الإلكترونية: الإفتراضية وإستراتيجية البحث عن المعلومات، جامعة منتوري، قسنطينة.

35. رايس، شيماء. **شبكات التواصل الاجتماعي ودورها في ترقية خدمات المعلومات بالمكتبات الرئيسية للمطالعة العمومية الجزائرية: دراسة تحليلية. أطروحة دكتوراه.** تخصص: علم المكتبات.عنابة: جامعة باجي مختار، 2021.

36. مسوس، كمال. **نحو حوكمة نظم المعلومات في مؤسسات التعليم العالي: دراسة حالة عينة من مؤسسات التعليم العالي**. أطروحة دكتوراه. تخصص: تسيير عمومي. جامعة الجزائر 3، 2018.

❖ مقالات ودوريات علمية

37. عظيمي، أحمد؛ زغنوف،عبد الغني. **المعلومة وأهميتها في المجتمع المعلوماتي**. مجلة البحوث والدراسات الإنسانية. المجلد،08. العدد،09، 2014.

38. حازم يحي، منى. **أثر حوكمة المعلومات في تعزيز المستوى التعليمي لطلبة الدراسات الأولية والدراسات التطبيقية**. مجلة الآداب. المجلد،132.، 2020.

39. بركات، عبد الرزاق، بن حاوية، أمينة. **حوكمة تكنولوجيا المعلومات واليات تنفيذها وتقييمها في المكتبات**. مجلة العلوم الاجتماعية والإنسانية. المجلد،22. العدد،02، 2021.

40. حازم يحي، منى. **أثر حوكمة المعلومات في تعزيز المستوى التعليمي لطلبة الدراسات الأولية والدراسات التطبيقية**. مجلة الآداب. المجلد،132.، 2020.

41. بركات، عبد الرزاق؛ حاوية، أمينة. **حوكمة تكنولوجيا المعلومات: وسيلة للتحكم في مشاريع تكنولوجيا المعلومات في المكتبات الجامعية**. مجلة الناصرية للدراسات الاجتماعية والتاريخية. المجلد،12. العدد،02، 2021.ص 570

42. بن عمر، محمد البشير؛ دادن، عبد الغني. **حوكمة المؤسسات ودورها في تحسين أداء المؤسسة**. مجلة الدراسات الاقتصادية والمالية. المجلد،01. العدد،07، 2014.

43. عبد الدايم أحمد الحداد، نبيلة. **متطلبات تحقيق الامن السيبيراني في المكتبات الجامعية اليمنية**. مجلة جامعة البيضاء. المجلد، 04. العدد، 02، 2022.

44. إسمحان، منى عبد الله صال. **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**. مجلة كلية التربية بالمنصورة. المجلد، 01. العدد، 02، 2020.

45. بلبكاي، جمال. **المكتبات الجامعية والتقنية**. مجلة الحكمة للدراسات الاجتماعية. المجلد، 04. العدد، 07، 2016. .

46. يعقوب عادل، ناصر الدين. **إطار نظري مقترح لحوكمة الجامعات ومؤشرات تطبيقها في ضوء متطلبات الجودة الشاملة**. مجلة تطوير الأداء الجامعي. المجلد، 01. العدد، 02، 2012.

47. سرير عبد الله، ناذير ؛ رحمونة، بوشتة. **حوكمة المعلومات والوثائق في المؤسسات وأزمة كورونا**. مجلة الاقتصاد والتنمية البشرية. المجلد.12، العدد،02، 2021.

48. غالم جلطي، العربي بوزيان. **مفهوم الحوكمة: عوامل ظهورها ومرتكزاتها، ومجالات استخداماتها**. مجلة المالية والأسواق. المجلد،08. العدد،92، 2021.

49. رايس، عبد الوهاب؛ صغيري، ميلود. **درجة وعي موظفي المكتبات بمفهوم إدارة مخاطر امن المعلومات في المكتبات الجامعية: دراسة ميدانية بمكتبات جامعة محمد خيضر بسكرة**. مجلة العلوم الإنسانية. المجلد، 24. العدد، 02، 2024.

50. شرقي، فتيحة؛ قموح، فتيحة. **حفظ الأرشيف في الجزائر بين الحمية القانونية والإجراءات الفنية**. مجلة الاتحاد العربي للمكتبات والمعلومات. المجلد، 02. العدد، 09، 2009. ص 09: تاريخ الاطلاع 30 – 07 -2024

51. حميدي، حياة؛ طايلب، نسيمة. **مدخل مفاهيمي حول الامن السيبيراني**. مدار للدراسات للاتصالات والرقمية. المجلد،02. العدد، 02، 2022. ص 05

52. السمحان، منعبد الله بن صالح. **متطلبات تحقيق الأمن السيبيراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**. مجلة كلية التربية. العدد، 111، 2020. ص 08

53. الخضر،دلال؛ بن ديلمي،إسماعيل. **المورد البشري خطر أم حصن للمنظمة؟ مدخل إلى أمن المعلومات في ظل الذكاء الاقتصادي**، مجلة الافاق للدراسات الاقتصادية. المجلد، 05. العدد، 01، 2020. ص 126

54. شنافي، كفية. **آليات ومبادئ الحوكمة في شركات التأمين: دراسة مقارنة بين الشركة الجزائرية للتأمينCAAR وشركة AXA**. مجلة كلية بغداد للعلوم الاقتصادية. العدد، 45، 2015.

55. التيماني،مداخل زيد عبد الرحيم. **واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبيراني. مجلة الخدمة الاجتماعية**، العدد 67، 2021.

56. كادي، زين الدين؛ غوار، عفيف. **إدارة الجودة الشاملة ومعايير الايزو في المكتبات الجامعية الجزائرية: دراسة ميدانية بالغرب الجزائري**. مجلة الحضارة الإسلامية. المجلد، 05. العدد، 04، 2014.

57. بن سيدهم، حرية. **الأمن الفضائي السيبيراني: التحديات والحلول**. مجلة الجزائرية للأمن الإنساني. المجلد، 05. العدد، 02، 2020.

58. بوقرص، ساعد. **الأمن السيبيراني: مخاطر وتحديديات وتحديات تتطلب ممارسات وتوصيات وإستراتيجيات خاصة**. Journal of social protection research. المجلد، 03. العدد،01، 2022.

59. رايس، شيماء؛ فريحة ، محمد كريم. **الحضور الرقمي للمكتبات العامة في الفضاء السيبيراني من وجهة نظر مسيري المنصات التفاعلية: استطلاع اراء القائمين على حسابات المكتبات العامة الجزائرية بموقع فيسبوك**. مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–. المجلد، 35. العدد، 01، 2021.

60. بارشيد، ناهد عبد الله؛ عبيد راوية رضا. **أثر الإستراتيجية الوطنية للأمن السيبيراني في الحد من مخاطر نظم المعلومات المحاسبية: دراسة ميدانية على القطاعات الحكومية السعودية**. مجلة إدارة المخاطر والأزمات، المجلد،06، 2025.

61. فردي، لخضر. **المكتبات الجامعية في ظل مجتمع المعلومات: نحو التكيف مع التحديات**. مجلة العلوم الإنسانية: مجلد أ، العدد 28، 2007.

62. عواد، مايا حفيظ. **التحول الرقمي في المكتبات الجامعية: إستخدام التقنيات الحديثة لتطوير المناهج التعليمية**. المجلة العربية للنشر العلمي. العدد الثامن والسبعون، 2025.

63. بن عميرة، عبد الكريم. **سبل التعاون بين المكتبات جزائرية في العصر الرقمي وتوظيفها في العملية التعليمية: دراسة نظرية**. مجلة الأمير عبد القادر للعلوم الإسلامية. المجلد 36، العدد 02، 2022.

64. بوزارة، أحلام. **تعزيز مرئية الجامعات الجزائرية من خلال المكتبات الجامعية: دراسة حالة المكتبات المركزية في جامعة جيلالي اليابس سيدي بلعباس وجامعة فرحات عباس سطيف 1**. المجلة المغاربية للدراسات التاريخية. المجلد، 16. العدد،02، 2024.ص293-294

65. كوار، فوزية. **الخدمة المرجعية في المكتبات الجامعية الجزائرية**. مجلة الحضارة الإسلامية. المجلد، 1، العدد 28، 2016.ص.626

66. حمودي، سارة. **الخبرات المهنية للعاملين بالمكتبات الجامعية ودورها في تطوير الخدمات: من أجل توصيف المهام بمكتبة جامعة الجزائر 1**. مجلة دراسات وأبحاث. العدد 25، 2016،

67. نابتي، محمد صالح. **الوصول الى المعلومات العلمية والتقنية: واقع المكتبات الجامعية الجزائرية**. مجلة المكتبات والمعلومات. المجلد، 04. العدد، 01، 2011.

68. بومعرافي، بهجة. عقابو، خالد. **حماية الكيانات الرقمية وضمان استمراريتها من خلال استراتيجيات أمن المعلومات بالمستودعات الرقمية الجامعية: مستودع جامعة محمد خيضر بسكرة نموذجا**. مجلة المعيار. المجلد، 27. العدد، 03، 2023.

69. أبو موسى، أحمد عبد السلام. **مخاطر أمن نظم المعلومات المحاسبية الالكترونية: دراسة ميدانية على المنشآت السعودية**. مجلة الإدارة العامة. المجلد، 44. العدد، 03، 2024.

70. زيوش، زيوش. تيتلة، سارة. **نحو حوكمة الكترونية أفضل في المكتبات ومراكز المعلومات: دراسة تحليلية مقارنة بين لطار COBIT وباقي الأطر**. مجلة المعيار. المجلد، 29. العدد، 01، 2024.

71. بارة سميرة. **الأمن السيبيراني في الجزائر: السياسات والمؤسسات**. المجلة الجزائرية لأمن الإنساني. المجلد، 02. العدد، 02،2017.

72. خليفة، أحمد. ضيف الله، محمد هادي. واخرون. **أثر حوكمة تكنولوجيا المعلومات على الحد من المخاطر نظام المعلومات المحاسبي: دراسة ميدانية لعينة من المحاسبين من 2019/09/14 الى 2019/10/30**. مجلة الدراسات المالية والمحاسبية والإدارية. المجلد،08. العدد، 01، 2021

73. بنور، زينب. **الاليات القانونية لحماية قواعد البيانات في البيئة الرقمية**. مجلة القانون والعلوم السياسية. المجلد،10. العدد،02، 2024.

74. حزام، فتيحة. **حماية الأنظمة الرقمية بين الأليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 05-20**. مجلة الحقوق والعلوم الإنسانية. العدد، 03، 2020.

75. مسوس، كمال. حديد، نوفل. **مقاربة حماية أنظمة معلومات المؤسسة من الاعتداءات الالكترونية**. مجلة المؤسسة. المجلد، 05. العدد، 05، 2016.

76. نجاري بن حاح علي. فايزة. **جريمة التجسس الالكتروني**. مجلة دراسات الدفاع والاسقبالية. المجلد، 01. العدد، 11، 2019.

77. عادل نبيل، شحات علي. **تقنيات أمن وحماية المعلومات الرقمي للمستودع الرقمي للرسائل الجامعية المصرية**. مجلة كلية الآداب. المجلد، 01. العدد، 48، 2017.

78. داودي، منصور. مرابط، حمزة. **التشفير كآلية لحماية المصنفات الرقمية من القرصنة الالكترونية**. مجلة الحقوق والعلوم السياسية. المجلد، 10. العدد،01، 2023.

79. غربي، أحمد. قاسيمي، حورية. **دور سياسة التشفير الاليكتروني في حماية نظم معلومات الإدارة الالكترونية**. مجلة الاقتصاد الجديد. المجلد، 12. العدد، 01، 2021.

80. نقموش، عادل. **حوكمة المؤسسات ودورها في تحقيق جودة المعلومات المحاسبية**. مجلة البحث الاقتصاد الإداري. المجلد، 16. العدد، 02، 2022.

81. كداوة، عبد القادر. **تحديات المكتبات الجامعية في البيئة الرقمية: خدمات المعلومات أنموذجا**. مجلة المداد. المجلد، 04. العدد، 02، 2016.

82. بن برغوث، ليلى. **الامن السيبيراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات، واليات التصدي**. المجلة الدولية للاتصال الاجتماعي. المجلد، 10. العدد، 01، 2023.

83. كرمادي، شمس الدين، محمد كريم، فريحة. **واقع خدمات المعلومات بالمكتبات العامة في ظل تحديات البيئة الرقمية دراسة تحليلية: المكتبات العامة لولاية عنابة وسط**. المجلد، 26. العدد، 03، 2023.

84. زواوي، لمياء. رملي، فهيم. **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**. المجلة الجزائرية للأمن والتنمية. المجلد، 12. العدد، 02، 2023.

85. العيداني، محمد. **التهديدات السيبرانية وجرائم المعلومات**. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المجلد، 13. العدد، 01، 2024.

86. بوقنادل، عبد اللطيف. ماحي، أمين. **المكتبة الرقمية ودورها في تطوير البحث العلمي**. المجلة الجزائرية للعلوم القانونية والسياسية. المجلد، 57. العدد، 03، 2020.

87. كداوة، عبد القادر. **تأثير تكنولوجيا المعلومات على خدمات المكتبات الجامعية المركزية الجزائرية: جامعات الجزائر الوسط أنموذجا**. مجلة الدراسات والأبحاث، المجلد، 08. العدد، 24، 2016.

88. سعيدي، خليل. بن مهدي، مرزوق. **الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبيراني: واقع اليوم ورهان الغد**. مجلة السلام للعلوم الإنسانية والاجتماعية. المجلد، 06. العدد، 01، 2022.

89. سهلي، مراد. **توظيف تقنيات الذكاء الاصطناعي في تحسين أداء المكتبات الجامعية: دراسة ميدانية بالمكتبات الجامعية بجامعة محمد خيضر بسكرة**. مجلة دراسات وأبحاث. المجلد، 17. العدد، 01، 2025.

90. محمد كريم، فريحة. كرمادي، شمس الدين. **واقع خدمات المعلومات بالمكتبات العامة في ظل تحديات البيئة الرقمية دراسة تحليلية: المكتبات العامة لولاية عتابة وسط**. مجلة التواصل. المجلد، 26. العدد، 03، 2023.

91. الحسيني، فايزة. **الوعي بالأمن السيبيراني ترف أم ضرورة في عصر المعلوماتية**. مجلة البحث العلمي. المجلد، 13. العدد، 02، 2023.

92. . سليمان، محمد مصطفي. **حوكمة الشركات ودور أعضاء مجالس الإدارة والمديرين التنفيذيين**. دار الجامعة الإسكندرية. ط01، 2009.

93. بن قايد علي، محمد لمين. **حوكمة الشركات: نظام جديد للإدارة والرقابة**. مجلة البحوث في الحقوق والعلوم السياسية. المجلد، 08. العدد،01، 2002.

94. شنافة،جهرة؛ زرقاطة، مريم. **واقع حوكمة الشركات وسبل ارسائها في بيئة الأعمالالعربية**. مجلة مينا للدارسات الاقتصادية. المجلد، 02. العدد، 01، 2019.

95. . خليل، محمد. **دور المحاسب الإداري في إطار حوكمة الشركات**. مجلة الدراسات والبحوث التجارية. المجلد، 01. العدد، 02، 2003.

96. . إبراهيم، نرمين. **حوكمة البيانات والوثائق في إدارة جامعة الإسكندرية العامة**. المجلة العلمية للمكتبات والوثائق والمعلومات. المجلد، 04. العدد، 10، 2021.

97. إبراهيم، نرمين. **حوكمة البيانات والوثائق في إدارة جامعة الإسكندرية العامة**. المجلة العلمية للمكتبات والوثائق والمعلومات. المجلد، 04. العدد، 10، 2021.

98. . قوت، سهام. **إدارة البيانات الضخمة في الشركات التقنية: دراسة حالة شركتي google وMeta**. مجلة دراسات وأبحاث. المجلد، 15. العدد، 03، 2023.

99. بن عزوز، حاتم. **الأمن السيبيراني والجريمة الاليكترونية في الدول ما بعد الحداثية: الولايات المتحدة الأمريكية – نموذجا–**. مجلة الرسالة للدارسات الإعلامية. المجلد، 06. العدد، 02، 2022.

100. الشوابكة،عدنان عواد.**دور إجراءات امن المعلومات في الحد من مخاطر امن المعلومات في جامعة الطائف**. مجلة الدراسات والأبحاث. المجلد، 11. العدد، 04، 2019.

101. فيلالي، أسماء؛شليل، عبد اللطيف، **تهديدات امن المعلومات وسبل التصدي لها**، مجلة البشائر الاقتصادية. المجلد، 04. العدد، 02، 2019.

102. بوعيشة، بوغفالة؛ بلعيور، محمدنذير. **حماية الملكية الفكرية الأدبية والفنية في البيئة الرقمية في ظل التشريع الجزائري**. المجلد، 05. العدد، 05، 2020.

103. فردي، لخضر. **المكتبات الجامعية في ظل مجتمع المعلومات: نحو التكيف مع التحديات**. مجلة العلوم الإنسانية. المجلد، 18. العدد، 03، 2007.

104. عقابو، خالد؛ بومعرافي، بهجة. **حماية الكيانات الرقمية وضمان استمراريتها من خلال استراتيجيات امن المعلومات بالمستودعات الرقمية الجامعية: مستودع جامعة محمد خيضر بسكرة نموذجا**. مجلة المعيار. المجلد، 27. العدد، 03، 2023.

105. السعيد، سلوى. لبيب، ندىمصطفي. **حماية خصوصية بيانات المستفيدين في المكتبات الأكاديمية: مراجعة علمية للإنتاج الفكري**. مجلة الدولية لعلوم المكتبات والمعلومات. المجلد، 10. العدد، 03، 2023.

106. بن عبد الله الهزائي، نورة. **ضوابط ومتطلبات تطبيق الأمن السيبيراني لحماية البيانات في جامعة الأميرة نورة**. مجلة مكتبة الملك فهد الوطنية. المجلد 02. العدد، 28، 2023.

107. داود، مسعود. **الخدمات الرقمية للمكتبات العربية في ظل جائحة كوفيد 19 المكتبة المركزية بجامعة الجزائر 02 أنموذجا – دراسة تحليلية**. دراسات نفسية وتربوية. المجلد، 14. العدد، 02، 2021.

108. محاجبي، عيسى؛ زيرام، بهية. **إدارة الكفاءات في المكتبات الجمعية الجزائرية باعتماد مواصفة ايزو 9001: المكتبة المركزية لجامعة الجزائر 02 أبو القاسم سعد الله أنموذجا**. مجلة العلوم الاجتماعية والإنسانية. المجلد، 11. العدد، 02، 2021.

109. . كادي، زين الدين. **إجراءات الأمن والوقاية من الجرائم الاليكترونية في المكتبات ومراكز المعلومات**. مجلة الإشارة. المجلد، 03. العدد، 01.

110. . قارح، سماح. تسامده، حسان. **الابداع والابتكار في نظم وتكنولوجيا المعلومات: دراسة ميدانية لعينة من مكتبات الوسط الجزائري**. المجلة الجزائرية للعلوم الاجتماعية والإنسانية. المجلد، 09. العدد، 02، 2021.

111. . بن السبتي، عبد المالك. **تكنولوجيا المعلومات في المكتبات الجزائرية بين الرغبة والتغيير والصعوبات. مجلة علوم الاعلام والتكنولوجيا**. المجلد، 14. العدد، 01، 2004.

112. بعنوني، ليلي. **التهديدات في الفضاء السيبيراني وانعكاساتها على السيادة الرقمية: القرصنة الالكترونية نموذجا**. مجلة دراسات الدفاع والاستشراف. المجلد، 08. العدد،02، 2021.

113. . كاوجة، محمد الصغير. **الهجمات السيبرانية بين الواقع وسبل المواجهة**. مجلة الرسالة للدراسات الإعلامية. المجلد، 06. العدد، 03، 2022.

114. ميلود، ليفة. **أحكام الاتلاف الفيروسي للبرامج والبيانات الاليكترونية**. مجلة البحوث والدراسات. المجلد، 13. العدد، 02، 2016

115. . العيداني، محمد. **التهديدات السيبرانية وجرائم المعلومات**. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المجلد، 13. العدد، 01، 2024.

116. العيداني، محمد. **التهديدات السيبرانية وجرائم المعلومات**. مجلة الاجتهاد للدراسات القانونية والاقتصادية. المجلد، 13. العدد، 01، 2024.

117. بوخنفر، زوليخة. **إدارة الهوية الرقمية واشكالات السمعة والخصوصية والاختراق: العملاقة على الويب. الشبكات المعلوماتية**. مجلة الرقمنة للدراسات الإعلامية والاتصالية. المجلد، 03. العدد، 01، 2023.

118. حميل، مصطفى. **السيادة الرقمية: التحديات والحلول الهيكلية**. مجلة رقمنه للدراسات الإعلامية والاتصالية. المجلد، 02. العدد، 03، 2022.

119. رملي، فهمي؛ وزواوي، لمياء. **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**. المجلة الجزائرية للأمن والتنمية. المجلد، 12. العدد، 02، 2023.

120. رملي، فهمي؛ وزواوي، لمياء. **التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر**. المجلة الجزائرية للأمن والتنمية. المجلد، 12. العدد، 02، 2023.

121. إبراهيم أحمد، علياء. **دور الحوسبة السحابية في تطوير خدمات المعلومات في المكتبة الجامعية: دراسة حالة على المكتبة المركزية بجامعة الإمام عبد الرحمن بن فيصل**. مجلة الدراسات الجامعية للبحوث الشاملة. المجلد، 05. العدد، 33، 2024. ص 14769

122. السيد أحمد علي. منال. **تطبيقات تقنيات الذكاء الاصطناعي بالمكتبات الجامعية**. مجلة العربية الدولية. المجلد، 03. العدد، 03، 2023.

123. هندي عبد الله، أحمد. **استخدام الذكاء الاصطناعي في مجال المكتبات والمعلومات دراسة ببليومترية**. مجلة العلوم الإنسانية والاجتماعية. المجلد، 02. العدد، 03، 2022.

124. نيل، خيرة ؛صادوق، خضرة. **تطبيقات انترنيت الأشياء في المكتبات: دراسة نظرية**. مجلة الرواق للدراسات الاجتماعية والإنسانية. المجلد، 08. العدد، 02، 2022.

125. مقراني، قدور؛ عطايت الله، ربيع. **التحديات الأمنية لأنترنيت الأشياء**. المجلة الجزائرية للدراسات الاقتصادية والإدارية. المجلد، 01. العدد، 02، 2021.

126. خنوسي، كريمة. **الحماية الدولية من جرائم التقليد والقرصنة الإلكترونية وموقف المشرع الجزائري منها**. مجلة مصداقية. المجلد، 03. العدد، 03، 2021.

127. . حسين، عميروش؛ بلعسل بنت نبي، ياسمين.**التهديدات الالكترونية للأمن السيبيراني في الوطن العربي**. مجلة نوميروس الأكاديمية. المجلد، 02. العدد، 02، 2021.

128. حسين، عميروش؛ بلعسل بنت نبي، ياسمين.**التهديدات الالكترونية للأمن السيبيراني في الوطن العربي**. مجلة نوميروس الأكاديمية. المجلد، 02. العدد، 02، 2021.

129. شليل، عبد اللطيف. فيلالي، أسماء. **تهديدات أمن المعلومات وسبل التصدي لها**. مجلة البشائر الاقتصادية. المجلد، 04, العدد، 03، 2019.

130. مسوس، كمال؛ حديد، نوفيل. **العلاقة بين حوكمة نظم المعلومات وحوكمة المؤسسات وسيرورة تطبيقها بمؤسسات التعليمالعالي**. المجلة الجزائرية للعولمة والسياسات الاقتصادية. المجلد، 05. العدد، 01، 2014.

131. سلطان، إبراهيم. **نظم المعلومات الإدارية: مدخل النظم. الدار الجامعية**. الإسكندرية. ط، 01، 2005. ص 02_01

132. شعباني، مجيد؛ مزوار، منوبة. **حوكمة نظم المعلومات كألية لتدعيم الميزة التنافسية للمؤسسة**. مجلة العلوم التجارية. المجلد، 14. العدد، 02، 2015.

133. خلفلاوي، شمسضيات. **مفهوم إدارة المعلومات ومنهجية عملها**. مجلة الحقوق والعلوم الإنسانية. المجلد، 05. العدد، 01، 2012.

134. بودحاح. عبد الجليل. **التوجه نحو إدارة نظم معلومات حديثة في المنشأة – مدخل نظري–**. المجلة الجزائرية للدراسات المالية والمصرفية. المجلد، 02. العدد، 01، 2012.

135. غنيمات، رغد. **إدارة المعلومات والأرشفة الرقمية في المؤسسات الحكومية**. مجلة العربية للنشر العلمي. المجلد، 02. العدد، 41، 2022.

136. نعيمات، محمد خلود سليمان. **حذف الملفات المكررة والتخلص من البيانات والمعلومات المكررة**. المجلة العربية للنشر العلمي. المجلد، 02.. العدد، 50، 2022.

137. الخضر، أبو بكر سلطان محمد. **الميتاداتا بمواقع قواعد بيانات الوصول الحر في مجال علم المعلومات والمكتبات: دراسة تحليلية تقويمية**. مجلة التكامل في البحوث العلوم الاجتماعية والرياضية. المجلد، 05. العدد، 02، 2021.

138. بن محمد، هدى؛ كورتل، نجاة. **المعايير الدولية لإدارة أمن المعلومات**. المجلد، 20. العدد،02، 2023.

139. عقوق، شراف؛ دوفي، قرمية. **حوكمة الشركات ودورها في استقرار الأعمال**. مجلة الأصيل للبحوث الاقتصادية والإدارية. المجلد، 04. العدد، 02، 2020.

140. انتر، فارماكول. **حوكمة المعلومات: إدارة المخاطر، والامتثال**. المجلد، 06. العدد، 03، 2018.

141. .الشباطات، محمد علي. **مفهوم حوكمة الجامعات وأثره في تعزيز معايير الشفافية والمساءلة والمشاركة**. مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي. المجلد، 38. العدد، 02، 2018.

142. صمود سيد أحمد. لحمر خالد. **دور حوكمة الشركات في تطبيق مبدأ الإفصاح والشفافيةاتجاه المساهمين**. مجلة الدراسات الحقوقية. المجلد، 07. العدد، 02، 2020.

143. . يعقوب عادل، ناصر الدين. **إطار مقترح لحوكمة الجامعات ومؤشرات تطبيقها في ضوء متطلبات الجودة الشاملة**. مجلة تطوير الأداء الجامعي. المجلد، 01. العدد، 02، 2012.

144. السبيعي، فلاح بن فرج. **أثر تطبيق الشفافية الإدارية في الحد من الفساد الإداري في الشركات المالية السعودية**. المجلد، 37. العدد، 01، 2017.

145. بن فردية، محمد. **اليات حماية المعلومات والوثائق الإدارية دراسة من خلال أحكام الأمر 21-09**. المجلة الدولية للبحوث القانونية والسياسة. المجلد،05. العدد، 03، 2021.

146. أجعود، سعاد. **تجريم التعدي على سرية المعلومات والوثائق الادارية دراسة تحليلية على ضوء الأمر 21-09 المتعلق بحماية المعلومات والوثائق الإدارية**. مجلة الحقوق والعلوم الإنسانية. المجلد، 15. العدد، 02، 2022.

147. عباسي، محمد الحبيب. **الحماية الجزائية للمعلومات والوثائق الإدارية من خلال الأمر 21-09**. مجلة القانون والعلوم السياسية. المجلد، 09. العدد، 01، 2023.

148. الورفلي، طارق. **برنامج تدريس إدارة الوثائق والمحفوظات بجامعة الشرقية**. المجلد، 12. العدد، 02، 2020.

149. لطرش، حكيم. قوميد، فتيحة. **إدارة الوثائق الجارية والوسيطة: الأدوات والأساليب جامعة حسيبة بن بوعلي _ الشلف أنموذجا**. مجلة ببليوفيليا للدراسات المكتبات والمعلومات. العدد، 04، 2019.

150. قاشي، خالد. **نظام المعلومات التسويقية بالمؤسسة الاقتصادية الجزائرية**. مجلة الأبحاث الاقتصادية. العدد، 05، 2021.

151. . فيلالي، أسماء. **دور المواصفة الدولية ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات في المؤسسة**. مجلة إضافات إقتصاية. المجلد، 05، العدد 01، 2021.

152. مراد، كريم. خالد، شيروف. **نظام الأرشفة الإليكترونية SAE قراءة تحليلية في المصطلح والمفهوم**. مجلة المقدمة للدراسات الإنسانية والاجتماعية. المجلد، 07. العدد، 01، 2022.

153. شيماء، خالد شعبان محمد. **حوكمة الوثائق والمعلومات في المؤسسة والمتطلبات اللازمة لتطبيقها**. المجلة المصرية لعلوم المعلومات. المجلد، 11. العدد، 02، 2024.

154. الزميتي، أحمد فاروق علي. **واقع تطبيق مبادئ الحوكمة بجامعة العريش**. مجلة كلية التربية. المجلد،25. العدد، 25، 2019.

155. ترار، عبد الكريم. شيهاب، أنفال. **الاطلاع على الوثائق الإدارية في ظل الحماية القانونية**. مجلة علم المكتبات. المجلد، 14. العدد، 01، 2022.

156. صعصاع البديري، إسماعيل؛ عمار حنين، منصر. **دور الإدارة في الحفاظ على الوثائق في التشريع العراقي**. مجلة بابل للعلوم الإنسانية. المجلد، 28. العدد، 02، 2020.

157. أبو موسى، عبد السلام أحمد. **مخاطر أمن نظم المعلومات المحاسبية الإليكترونية دراسة ميدانية على المنشآت السعودية.** مجلة الإدارة العامة. المجلد، 44. العدد، 03، 2004.

158. مسوس، كمال. **ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الالكترونية.** المجلة الجزائرية للعولمة والسياسات الاقتصادية. المجلد،13، 2022.

159. قدايفة، أمينة. **استراتيجية أمن المعلومات.** مجلة أبعاد اقتصادية. المجلد، 06. العدد، 01، 2016.ص 166

160. بوضياف سهيلة، حمراني أمنة. **أمن المعلومات في الجزائر: الإجراءات والتحديات.** مجلة الجزائرية للأمن والتنمية. المجلد، 09. العدد، 16، 2020.

161. بوضياف، سهيلة؛ حمراني، أمنة. **أمن المعلومات في الجزائر: الإجراءات والتحديات.** مجلة الجزائرية للأمن والتنمية. المجلد، 09. العدد، 16، 2020.

162. بن عيدة، فوزية؛ بحوصي، رقية. **حوكمة البيانات في المؤسسات التعليم العالي: الآليات، والاستراتيجيات، العوائق.** المجلة المغاربية للمخطوطات. المجلد، 20. العدد، 01، 2024.

163. الميلبي، أروى النصار؛ الضحوي، هناء علي. **نضج إدارة البيانات الرئيسية في المؤسسات الحكومية: دراسة حالة لوزارة النقل والخدمات اللوجستية.** مجلة دراسات المعلومات والتكنولوجيا. المجلد، 01. العدد،03، 2023.

164. زياني، زهرة. بودية، فاطمة الزهراء. **تقييم الأداء في المؤسسات الخدمية باستخدام تحليل البيانات المغلفة: جامعة الشلف نموذجا.** مجلة بحوث الإدارة والاقتصاد. المجلد، 01. العدد، 02، 2019.

❖ ملتقيات ومؤتمرات علمية

165. العبدلية، رقية بنت خلفان بن ناصر. **تطبيقات حوكمة البيانات في سلطنة عمان.** المؤتمر والمعرض السنوي السادس والعشرين حول: التقنيات الناشئة وتطويرها في المكتبات والمؤسسات المعلومات. جمعية المكتبات المتخصصة؛ فرح الخليج العربي: الكويت، 2023.

166. قتاتلية، خولة.**الأمن السبراني ، التحديات والرهانات.** ملتقى وطني حول: دور الجامعة في تعزيز ثقافة الأمن السيبيراني.جامعة الجزائر 03، 2024.ص15

❖ مواقع إلكترونية

❖ مواقع عربية

167. الهيئة الوطنية للأمن السيبيراني: المملكة على الموقع:https://nca.gov.sa/ar/

168. الهيئة الوطنية للأمن والسلامة المعلومات. **سياسة النسخ الاحتياطي.** متاح على الرابط: **https://nissa.gov.ly**

169. تم الاطلاع بتاريخ: 06-01- 2025 على 19.35

170. الهيئة الوطنية لأمن وسلامة المعلومات National Information Security and Safety Authority. **السياسة الوطنية لأمن وسلامة المعلومات.** ص 65 تاريخ الولوج:13/03/ 2025.على 12:36 متاح على الرابط: https://nissa.gov.ly

171. موقع الجزيرة نت. **مقال حول: النسخ الاحتياطي وسيلة مثلى لحماية البيانات**. تاريخ الولوج: 13/ 03: 2025. على 13:06 متاح على الرابط: https://www.aljazeera.net

172. الجزيرة " الجزيرة نت". **تقنيات الأمن السيبيراني والتحديات المستقبلية**. تاريخ الولوج: 16-03-2025 على 20:30 متاح على الرابطwww.aljazeera.net

173. الجزيرة " الجزيرة نت". **قراءة في كتاب "الامن السيبيراني المخاطر والتحديات والمواجهة**. تاريخ الولوج: 16-03-2025 على 22:30 متاح على الرابطwww.aljazeera.net

174. الندوة الجهوية للشرق الجزائري. تاريخ الإطلاع: 25-12-2023، على الساعة: 14:45. متاح ع الرابط: /https://www.univ-constantine2.dz/cruest 6

❖ مواقع إلكترونية أجنبية

176. Iso/IEC27001: 2022.**Information Security**. **Cyber Security and privacy protection information security management systems requirements**. Https:// www.iso / standard/27001 .19:23h

177. Iso/IEC27001: 2022.**Information Security**. **Cyber Security and privacy protection information security management systems requirements**. Https:// www.iso / standard/27001 .19:23h

178. **Iso/IEC27001**: **2022**. Https://www.iso/standard/27001

179.National Cybersecurity centre of Excellence. **Identity and Access**. **Management** (**IAM**) **Cyber security**. Visit: 14/03/2025. 15:23. Constable on: https://www.nccoe.nist.gov

180.International protective service. **IPS Security**. Visit: 13/03/2025. 16 :34. Constable on https://ip.global.com

مراجع باللغة الإنجليزية

181.Makhlouf Shabou, Basma. **Information Governance**, **European Public Administrations**. Ala- Ica conference. Mexico City,28 November, 2017

182. ELzidi, Sulaiman. **Harnessing the power pf Artificial Intelligence Applications in Academic Library Information Services**. The Bibliography Journal for Library and Information studies. Vol,06. Nu,01, 2024. P 79

183. A. R François. **Manuel de l'organisation de l'entreprise**. Les Edition de l'organisation. N (07), 1988.

184. Makhlouf Shabou, Basma. **Information Governance**, **European Public Administrations**. Ala- Ica conference. Mexico City,28 November, 2017

185. Done White. John MC Manus. Andrew Atherton. **Governance and information**, **Governance some Ethical considerations within an expanding information Society**. University of Lincoln. Faculty of business and law: Brayford Pool. England, 2004.

186. Zahi, Jamal ;Belhaj,Aadil. **La gouvernance des technologies de l'information** : **un dispositif de contrôle du système d'information éducation**. Revue repères et perspectives économiques. V (02). N (02),

187. Uttam, Acharya. **Records management in documentaliste**. Revues Science de l'information. Vol (46). N (02), 2009

188. Zeroual, Sihem. Tadjine, Farida. **Good Governance and development**: **A Critical Analysis of the Relationship**. Revue critique de droit et science politiques. Vu (03). Nu (02), 2019.

189. Benkara Mostafa, Aicha. **Governance Of Personal Data Privacy in Algerian Legislation**. Revue Comparative legal studies. Vu (09). Nu (02), 2024.

190. Kaddouri, Ammar. **La relation des Risk management Et l'audit interne dans la Gouvernance des Epe.**Revue de recherche en finance et comptabilité. Vo (01). Nu (02),2016.

191. Chabani, Said. **Le Management de l'information Et la prise De Décisions En Entreprise**. La Revue de la communication et du journalisme. Vu (02). Nu (01), 2015.

192. Ben abdallâh, Ahceneyoucef. Boudour, Rachid. **Approche complète de développement des IPS pour les socs**. Synthes. Volume. 22, Numero,01, 2016.

193. Laura Dubois, Vivian Tero. **Practical information Governance**: **balancing cost**, **Risk and productivity**, IDC White Paper, 2010.

194. EL Qasmi, Mohamed Jaouad. Kriouile, Abdelaziz. **Le Management de l'information** : **Une Dimension Stratégique Et Organisationnelle**. Revue de l'information scientifique et technique. Vu (14). Nu (01),2004.

195.Tonia San Nicolas-Rocca. **Information Security in Libraries**: **Examining the Effects of Knowledge Transfer**. Information Technology and Libraries, Vol.38, N.02, 2019

196. Anderfuhren, Sandrine.Romagnoli, Patrizia.**La maturité de la gouvernance de l'information dans les administrations publiques européennes** : **la perception de la gouvernance de l'information dans l'administration publique genevoise**. Mémoire de recherche.Haute École de Gestion de Genève, 2018

قائمة الجداول

قـائمة الجداول

قـائمة الجداول

قـائمة الجداول

قائمة الأشكال

قـائمة الأشكال

قائمة الملاحق

الملحق رقم (01): إستمارة إستبيان قبل التحكيم

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد خيضر – بسكرة

كلية العلوم الإنسانيةوالاجتماعية

قسم العلوم الانسانية

شعبة علم المكتبات

تخصص المؤسسات الوثائقية

استمارة تحكيم استبيان

السلام عليكم ورحمة الله وبركاته؛

يقوم الباحث بإجراء دراسة حول: **أثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات الجامعية بالمكتبات الجامعية بالشرق الجزائري**. وذلك للحصول على درجة الدكتوراه في **تخصص المؤسسات الوثائقية في ظل التكنولوجيا الحديثة**. لذا ارجوا منكم التكرم بإبداء رأيكم السديد ومقترحاتكم بشان فقرات الاستبيان تقيس او لا تقيس؛ ومدى انتمائها للمجال المحدد لها؛ وبنائها اللغوي؛ واية اقتراحات او تعديلات ترونها مناسبة لتحقيق حدف الدراسة الحالية.

البيانات الشخصية:

1. **الاسم واللقب:**.....
2. **التخصص:**.....
3. **الدرجة العلمية:**.....
4. **الجامعة:**.....

إعداد الباحث:

عبد الوهاب رايس

قائـمة المـلاحق

شاكرين لكم حسن التعاون وبارك الله في جهودكم الطيبة لخدمة البحث العلمي.

المحور الاول: وعي اخصائي المعلومات بحوكمة المعلومات لمخاطر الامن السيبراني		العبارات	مدى قياس العبارات		مدى مناسبة الصياغة اللغوية للعبارات		ملاحظات المحكم
			تقيس	لا تقيس	مناسبة	غير مناسبة	
	1-	فهم المسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني.					
	2-	الفهمالمشترك بين اخصائي المعلومات لأهمية المسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الامن السيبراني.					
	3-	التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الامن السيبراني.					
	4-	حوكمة المعلومات هي مجموعة السياسات والإجراءات التي تُطبق في المكتبات الجامعية لتنظيم وإدارة المعلومات بهدف تقليل وتعزيز الحماية ضد المخاطر السيبرانية.					
	5-	مخاطر الأمن السيبرانيمن الناحية العملية على أنها التهديدات والثغرات المحتملة التي قد تؤثر سلبًا على سرية وسلامة وتوافر أنظمة المعلومات والبيانات داخل المكتبات الجامعية.					
	6-	الاطلاع بالشكل الكافي على الالتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة					
	7-	السياسات والاجراءات المتبعة في المكتبة تضمن حماية المعلومات والامتثال للمعايير القانونية والتنظيمية.					
	8-	اخصائي المعلومات ملتزمون بتطبيق السياسات والاجراءات المتعلقة بأمن المعلومات.					
	9-	ادراك اهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات					

	لمخاطر الامن السيبراني.						
10-	الدراية بالإجراءات وتقنيات الحفظ التي يجب اتباعها واستخدامها لحفظ المعلومات بطريقة امنة ينجح حوكمة المعلومات لمخاطر الامن السيبراني.						
المحور الثاني: حوكمة المعلومات	أولا: المـــــــسؤولية						
11-	توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة.						
12-	تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات فيالمكتبة.						
13-	تم تحديد المسؤوليات لحفظ وحذف المعلومات.						
14-	هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين.						
15-	يتم تنظيم دورات تدريبية متنوعة لضمان أن جميع العاملين يفهمون ويؤدون مسؤولياتهم بفعالية ضمن إطار حوكمة المعلومات، مما يعزز من الأمان والامتثال داخل المكتبات الجامعية.						
16-	تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان التزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والامتثال للمعايير والسياسات.						
	ثـــــــانيا: الامتـــــــثال						
17-	تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية						
18-	يتم تنفيذ إجراءات في الكشف عن أي مخالفات أو عدم تطابق، مع المعايير الداخلية والخارجية؛ مما يسمح باتخاذ الإجراءات التصحيحية اللازمة للحفاظ على مستوى عالٍ من الامتثال والجودة".						
19-	تتبنى المكتبة استراتيجية لإدارة مخاطر عدم الامتثال						
20-	توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الامتثال وتوضيح المعايير والممارسات المطلوبة						

21-	الرقابة المستمرة للاداء والاجراءات خلال تنفيذ الانشطة اليومية لضمان الالتزام الفوري للموظفين بالسياسات لمنع والمشكلات قبل ان تحدث					
22-	يتم اجراء مراجعات دورية لتقييم منتظم للوائح والاجراءات لضمان التزامها بالمعايير بمرور الوقت .					
ثـالثـــا:الحـــــــــفظ						
23-	تلتزم المكتبة بمبدأ الحفاظ على المعلومات للفترة الزمنية اللازمة وفقًا للمتطلبات القانونية والتنظيمية					
24-	تستخدم المكتبة (الوسائل ؛ مواد؛ برمجيات)للحفظ الامن؛وارشفة المعلومات					
25-	تتبع المكتبة سياسات واجراءات لحفظ المعلومات والحفاظ على سلامتها واستمراريتها وبشكل صحيح ومنظم					
26-	تتم مراجعة وتحديث سياسات حفظ المعلومات بانتظام وفقا للمتطلبات القانونية والتنظيمية والتشغيلية.					
27-	تسنخدم المكتبة تقنيات الارشفة الملائمة للمحافظة على المعلومات بشكل دائم					
28-						
رابـــــــــعا:الاستـــــــبعاد						
29-	يتم استبعاد المعلومات المتعلقة بمصادر المعلومات والمعطيات الشخصية بشكل منتظم وفقا للسياسات والمتطلبات القانونية					
30-	يتم الاستبعاد تلقائيا للمعلومات المخزنة الكترونيا بشكل نهائي من وسائل الاتاحة.					
31-	تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات.					
32-	توفر المكتبة برامج للتوعية والتدريب المستمر بشان ترتيبات المصير النهائي للمعلومات					
33-	توثق المكتبة جميع الاجراءات المتعلقة بترتيبات المصير النهائي للمعلومات.					

	34-	يتم تقييم مدى التزام المكتبة بسياسات الاستبعاد وتحسين فعالية الاجراءات المتبعة.						
المحور الثالث : مخاطر الأمن السيبراني		أولا: المخاطر المتعلقة بالسرية						
	35-	هجمات التنصت (اعتراض شبكة الاتصالات او التقاط البيانات اثناء نقلها داخل وخارج المكتبة).						
	36-	هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام او المنقولة عبر الشبكة).						
	37-	الوصول غير المصرح به لنظام المكتبة من قبل اطراف خارجية مثل المهاجمين						
	38-	الوصول غير المصرح به لنظام المكتبة من قبل اطراف داخلية مثل المكتبيين(الموظفين)						
	39-	الافعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة).						
	40-	الافعال المتعمدة المتعلقة بالابتزاز(الابتزاز بالكشف عن المعلومات).						
	41-	هجمات الاصطياد الالكتروني؛ انتحال هوية اشخاص او منظمة يثق بهم الضحية باستخدام وسائل تقنية.						
	42-	هجمات الهندسة الاجتماعية (القدرة على التمثيل واقناع الضحية بالإفصاح عن المعلومات السرية).						
		ثـــــانيا:المخاطر المتعلقة بالسلامة						
	43-	الادخال الغير متعمد للبيانات الخاطئة من قبل الموظفين						
	44-	اتلاف البيانات غير متعمد من قبل الموظفين						
	45-	اتلاف البيانات المتعمد من قبل الموظفين						
	46-	الادخال المتعمد للبيانات الخاطئة من قبل الموظفين .						
	47-	اخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين اثناء كتابة البرامج.						
	48-	التقادم التكنولوجي مثل الاجهزة والانظمة المتقادمة.						
		ثـالثـــا:المخاطر المتعلقة بالتوافر						

49-	هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول الى الخدمة).						
50-	تفجير البريد الالكتروني (اغراق بريد المكتبة بالرسائل مما يؤدي الى توقفه عن العمل).						
51-	الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف.						
52-	اعطال اجهزة النظام الفنية.						
53-	اعطال معدات الشبكة الفنية.						
54-	انقطاع شبكة الإنترنت أو ضعف الاتصال بالشبكة بما يؤثر على إتاحة الخدمات الرقمية واستمراريتها.						
رابـــــــعا:المخـــاطر العـــــــــامة							
55-	قرصنة الهاتف (اجراء مكالمات مجانية؛ او الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .)						
56-	هجمات الانتحال مثل انتحال عنوانIP؛ او البريد الالكتروني؛ او موقع الويب؛ او هوية المتصل.						
57-	فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).						
58-	ديدان الحاسوب(قادرة على استنساخ نفسها تلقائيا).						
59-	احصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله).						
60-	برامج التجسس الالكتروني(برامج خفية تراقب استخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم).						
61-	القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدا بتدمير المعلومات).						
62-	هجمات الرسائل المزعجة او الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل.						

المحور الثاني	أولا وضوح السياسات الداخلية ومسؤوليات الأفراد فيما يتعلق بإدارة البيانات الحساسة. (إدارة إطار الحوكمةCOBIT 5: APO01)؛ISO 27001 A.6 (تنظيم أمن المعلومات)

63 –	عندما تكون المسؤوليات موزعة بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة. هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به، حيث يتم تطبيق تدابير تحكمية دقيقة تحد من عدد الأشخاص الذين لديهم إمكانية الوصول إلى البيانات الحساسة.					
64 –	توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها. هذا يسهم في تعزيز سلامة البيانات، حيث أن كل عملية تعديل تُراجع وتُعتمد من قبل المسؤولين المعنيين.					
65 –	وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية.					
ثـــــانيا: تكامل سياسات المكتبة مع التشريعات والمعايير العالمية للأمن السيبراني. () COBIT 5: MEA03ضمان الامتثال)؛() ISO 27001: A.18 الامتثال)؛(الامتثال وإدارة المخاطرITIL)						
66 –	الامتثال للقوانين والتشريعات مثل GDPR وغيرها من المعايير العالمية يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة، ما يقلل من فرص التسريب أو الاختراق.					
67 –	الامتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية مثل التشفير، التحقق متعدد العوامل، والتحديثات الأمنية الدورية، مما يحافظ على سلامة البيانات ويمنع التلاعب بها.					
68 –	تتطلب التشريعات غالبًا خططًا للطوارئ واستمرارية الأعمال. الامتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الانقطاع غير المخطط له.					
ثـالثـــا: كفاءة نظام إدارة دورة حياة البيانات . () COBIT 5: DSS06إدارة استمرارية الأعمال)؛ ISO 27001: A.8 (إدارة الأصول)						
69 –	سياسات الحفظ التي تشمل عمليات مراجعة وتدقيق دورية تساهم في الحفاظ على سلامة البيانات، حيث تتيح التعرف على أي تغييرات غير مصرح بها أو تلف قد يحدث للبيانات على المدى الطويل.					

70 –	ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة التي قد تعيق الوصول الفعّال إلى المعلومات الهامة، مما يحسن من توافر البيانات الضرورية.					
71 –	تطبيق سياسات الحفظ السليمة يضمن أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للاختراقات					
رابـــــــــعا: فعالية وأمان عمليات استبعاد البيانات الحساسة. COBIT 5: DSS06 (إدارة استمرارية الأعمال) DSS02إدارة خدمة الأمن(؛) ISO 27001: A.8 إدارة الأصول) و) A.11التحكم في الوصول(؛)ITIL إدارة الطلب والحوادث(						
72 –	إجراءات الاستبعاد المطبقة بشكل صحيح تضمن أن البيانات الحساسة لا يمكن استعادتها بعد الحذف، مما يحميها من الاستخدام غير المشروع ويضمن بقاء المعلومات الخاصة تحت السيطرة الكاملة.					
73 –	تنفيذ عمليات الاستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية.					
74 –	الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة.					

الملحق الثاني: إستمارة إستبيان النهائية

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد خيضر – بسكرة

كلية العلوم الإنسانيةوالاجتماعية

قسم علم المكتبات

استبيان أطروحة دكتوراه ل م د تحت عنوان:

أثر حوكمة المعلومات على مخاطر الأمن السيبراني بالمكتبات الجامعية بالشرق الجزائري: دراسة على عينة من المكتبات الجامعية

إعداد الطالبة:إشر اف الأستاذ(ة)

عبد الوهاب رايس ميلود صغيري

نضع بين ايديكم هذا الاستبيان والذي يهدف الى دراسة: اثر حوكمة المعلومات على مخاطر الامن السيبراني .

ولهذا نرجو من سيادتكم الاجابة على الاسئلة من خلال وضع علامة (X) في المكان المناسب؛ مع العلم ان هاته المعلومات لن تستخدم الا في اطار علمي بحت ؛ شاكرين لكم حسن تعاونكم.

السنة الجامعية :2025/2024

قائـمة المـلاحق

أولا: البيانات الشخصية:

1- **الجنس:** ذكر ☐ أنثى ☐

2- **جامعة العمل:** قسنطينة2 ☐ عنابة ☐ بالمة ☐ تنة1 ☐ الأمير عبد القادر ☐ بسة ☐

بسكرة ☐ سطيف1 ☐ سكيكدة ☐ نة3 ☐ ال ☐ بريريج ☐ سط ☐

الوادي ☐ جل ☐ لة ☐ ة ☐ طينة1 ☐ باتنة2 ☐ اهراس ☐ ام ☐

البواقي ☐ لة ☐

3- **المستوى العلمي :**

دكتوراه ☐ ستر ☐ ل ☐ د ☐ تطبيقية ☐ ☐ الثالثة ثانوي ☐

خارج التخصص:.....

4- **الرتبة:**

- رئيس محافظي المكتبات الجامعية ☐
- محافظ المكتبات الجامعية ☐
- ملحق بالمكتبات الجامعية من المستوى الاول ☐
- ملحق بالمكتبات الجامعية من المستوى الثاني ☐
- مساعد بالمكتبات الجامعية ☐
- عون تقني بالمكتبات الجامعية ☐

5- **الخبرة المهنية :**

- اقل من 5 سنوات ☐
- من 5 إلى 10 سنوات
- من 10 إلى 15 سنة ☐

- من 15 إلى 20 سنة ☐
- أكثر من 20 سنة ☐

المحور الاول: وعي اخصائي المعلومات بحوكمة المعلومات لمخاطر الامن السيبراني

المحور الاول: وعي اخصائي المعلومات بحوكمة المعلومات لمخاطر الامن السيبراني		الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	1-	فهم المسؤوليات الفردية فيما يتعلق بحماية المعلومات الحساسة يسهم في حوكمة المعلومات لمخاطر الامن السيبراني.					
	2-	الفهمالمشترك بين اخصائي المعلومات لأهمية المسؤولية الجماعية في الحفاظ على أمن المعلومات داخل المكتبة يقلل من مخاطر الامن السيبراني.					
	3-	التدريب والتوعية حول كيفية تنفيذ المسؤوليات فيما يتعلق بحوكمة المعلومات يسهم في التقليل من مخاطر الامن السيبراني.					
	4-	حوكمة المعلومات هي مجموعة السياسات والإجراءات التي تُطبق في المكتبات الجامعية لتنظيم وإدارة المعلومات بهدف تقليل وتعزيز الحماية ضد المخاطر السيبرانية.					
	5-	مخاطر الأمن السيبراني من الناحية العملية على أنها التهديدات والثغرات المحتملة التي قد تؤثر سلبًا على سرية وسلامة وتوافر أنظمة المعلومات والبيانات داخل المكتبات الجامعية.					
	6-	الاطلاع بالشكل الكافي على الالتزامات القانونية المرتبطة بحوكمة المعلومات في المكتبة					
	7-	السياسات والاجراءات المتبعة في المكتبة تضمن حماية المعلومات والامتثال للمعايير القانونية والتنظيمية.					
	8-	اخصائي المعلومات ملتزمون بتطبيق السياسات والاجراءات المتعلقة بأمن المعلومات.					
	9-	ادراك اهمية حفظ المعلومات بطريقة تضمن حمايتها من الوصول غير المصرح به يسهم بحوكمة المعلومات لمخاطر الامن السيبراني.					

	10-	الدراية بالإجراءات وتقنيات الحفظ التي يجب اتباعها واستخدامها لحفظ المعلومات بطريقة امنة ينجح حوكمة المعلومات لمخاطر الامن السيبراني.				

المحور الثاني: مستوى حوكمة المعلومات بالمكتبات الجامعية محل الدراسة

المحور الثاني: حوكمة المعلومات		أولا: المـــــــسؤولية	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	11-	توجد سياسات وإجراءات واضحة وموثقة للمسؤولية عن المعلومات في المكتبة.					
	12-	تحدد هذه السياسات الأدوار والمسؤوليات المتعلقة بإدارة وحماية المعلومات فيالمكتبة.					
	13-	تم تحديد المسؤوليات لحفظ وحذف المعلومات.					
	14-	هناك تفويض واضح لمسؤولية تسير الملفات والمعلومات إلى الأشخاص المناسبين.					
	15-	يتم تنظيم دورات تدريبية متنوعة لضمان أن جميع العاملين يفهمون ويؤدون مسؤولياتهم بفعالية ضمن إطار حوكمة المعلومات، مما يعزز من الأمان والامتثال داخل المكتبات الجامعية.					
	16-	تعزيز ثقافة المسؤولية الشخصية بين العاملين لضمان التزامهم بالممارسات الأمنية وتحملهم المسؤولية عن حماية المعلومات والامتثال للمعايير والسياسات.					
		ثـــــانيا: الامتـــــــثال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	17-	تلتزم المكتبة بالتشريعات واللوائح والمعايير ذات صلة بحوكمة المعلومات والخصوصية					
	18-	يتم تنفيذ إجراءات في الكشف عن أي مخالفات أو عدم تطابق، مع المعايير الداخلية والخارجية؛ مما يسمح باتخاذ الإجراءات التصحيحية اللازمة للحفاظ على مستوى عالٍ من الامتثال والجودة".					
	19-	تتبنى المكتبة استراتيجية لإدارة مخاطر عدم الامتثال					
	20-	توفر المكتبة برامج تدريبية للموظفين لزيادة الوعي بأهمية الامتثال وتوضيح المعايير والممارسات المطلوبة					
	21-	الرقابة المستمرة للاداء والاجراءات خلال تنفيذ الانشطة اليومية لضمان الالتزام الفوري للموظفين بالسياسات لمنع والمشكلات قبل ان تحدث					
	22-	يتم اجراء مراجعات دورية لتقييم منتظم للوائح والاجراءات لضمان التزامها بالمعايير بمرور الوقت .					
		ثـالثـــا:الحـــــــــفظ	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة

-23	تلتزم المكتبة بمبدأ الحفاظ على المعلومات للفترة الزمنية اللازمة وفقًا للمتطلبات القانونية والتنظيمية					
-24	تستخدم المكتبة (الوسائل ؛ مواد؛ برمجيات)للحفظ الامن؛وارشفة المعلومات					
-25	تتبع المكتبة سياسات واجراءات لحفظ المعلومات والحفاظ على سلامتها واستمراريتها وبشكل صحيح ومنظم					
-26	تتم مراجعة وتحديث سياسات حفظ المعلومات بانتظام وفقا للمتطلبات القانونية والتنظيمية والتشغيلية.					
-27	تسنخدم المكتبة تقنيات الارشفة الملائمة للمحافظة على المعلومات بشكل دائم					
-28	تطبق المكتبة إجراءات النسخ الاحتياطي الدوري واختبار الاسترجاع لضمان استمرارية المعلومات وإتاحتها عند الحاجة.					
	رابـــــــعا:الاستـــــــبعاد	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
-29	يتم استبعاد المعلومات المتعلقة بمصادر المعلومات والمعطيات الشخصية بشكل منتظم وفقا للسياسات والمتطلبات القانونية					
-30	يتم الاستبعاد تلقائيا للمعلومات المخزنة الكترونيا بشكل نهائي من وسائل الاتاحة.					
-31	تستخدم المكتبة نظام تصنيف المعلومات لتحديد الترتيبات المناسبة للمصير النهائي للمعلومات.					
-32	توفر المكتبة برامج للتوعية والتدريب المستمر بشان ترتيبات المصير النهائي للمعلومات					
-33	توثق المكتبة جميع الاجراءات المتعلقة بترتيبات المصير النهائي للمعلومات.					
-34	يتم تقييم مدى التزام المكتبة بسياسات الاستبعاد وتحسين فعالية الاجراءات المتبعة.					

المحور الثالث : مستوى مخاطر الامن السيبراني بمكتبات محل الدراسة

المحور الثالث : مخاطر الامن السيبراني		**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
	أولا: المخاطر المتعلقة بالسرية					
-35	هجمات التنصت (اعتراض شبكة الاتصالات او التقاط البيانات اثناء نقلها داخل وخارج المكتبة).					
-36	هجمات كسر كلمة المرور(الوصول الى كلمة المرور المخزنة في النظام او المنقولة عبر الشبكة).					
-37	الوصول غير المصرح به لنظام المكتبة من قبل اطراف خارجية مثل المهاجمين					
-38	الوصول غير المصرح به لنظام المكتبة من قبل اطراف داخلية مثل المكتبيين(الموظفين)					

39-	الافعال المتعمدة المتعلقة بالسرقة (معدات او معلومات المكتبة).					
40-	الافعال المتعمدة المتعلقة بالابتزاز(الابتزاز بالكشف عن المعلومات).					
41-	هجمات الاصطياد الالكتروني؛ انتحال هوية اشخاص او منظمة يثق بهم الضحية باستخدام وسائل تقنية.					
42-	هجمات الهندسة الاجتماعية (القدرة على التمثيل واقناع الضحية بالإفصاح عن المعلومات السرية).					
	ثـــــانيا:المخاطر المتعلقة بالسلامة	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
43-	الادخال الغير متعمد للبيانات الخاطئة من قبل الموظفين					
44-	اتلاف البيانات غير متعمد من قبل الموظفين					
45-	اتلاف البيانات المتعمد من قبل الموظفين					
46-	الادخال المتعمد للبيانات الخاطئة من قبل الموظفين .					
47-	اخطاء البرمجيات الفنية مثل الاخطاء التي يقع فيها المبرمجين اثناء كتابة البرامج.					
48-	التقادم التكنولوجي مثل الاجهزة والانظمة المتقادمة.					
	ثـالثـــا:المخاطر المتعلقة بالتوافر	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
49-	هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول الى الخدمة).					
50-	تفجير البريد الالكتروني (اغراق بريد المكتبة بالرسائل مما يؤدي الى توقفه عن العمل).					
51-	الكوارث الطبيعية مثل الحرائق؛ الصواعق؛ والعواصف.					
52-	اعطال اجهزة النظام الفنية.					
53-	اعطال معدات الشبكة الفنية.					
54-	انقطاع شبكة الإنترنت أو ضعف الاتصال بالشبكة بما يؤثر على إتاحة الخدمات الرقمية واستمراريتها.					
	رابـــــــعا:المخـــاطر العـــــــــامة	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
55-	قرصنة الهاتف (اجراء مكالمات مجانية؛ او الوصول غير المشروع الى المعلومات؛ او تعطيل الخدمة .)					
56-	هجمات الانتحال مثل انتحال عنوانIP؛ او البريد الالكتروني؛ او موقع الويب؛ او هوية المتصل.					
57-	فيروسات الحاسوب(تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).					
58-	ديدان الحاسوب(قادرة على استنساخ نفسها تلقائيا).					

	-59	احصنة طروادة(برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المعد عند تفعيله).					
	-60	برامج التجسس الالكتروني(برامج خفية تراقب استخدام الحاسوب ومع المعلومات عن المستخدم وارسالها للمهاجم).					
	-61	القنبلة المعلوماتية (برنامج معين يضل ساكن حتى تاريخ محدد او ظهور حدث معين ثم يبدا بتدمير المعلومات).					
	-62	هجمات الرسائل المزعجة او الغير مرغوب فيها مثل رسائل الهاتف القصيرة؛ او البريد الالكتروني؛ او مواقع التواصل.					

المحور الرابع : اثر حوكمة المعلومات على مخاطر الامن السيبراني بالمكتبات الجامعية محل الدراسة

المحور الرابع : اثر حوكمة المعلومات على مخاطر الامن السيبراني		أولا وضوح السياسات الداخلية ومسؤوليات الأفراد فيما يتعلق بإدارة البيانات الحساسة. (إدارة إطار الحوكمةCOBIT 5: APO01)؛ ISO 27001 A.6(تنظيم أمن المعلومات)	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	-63	عندما تكون المسؤوليات موزعة بوضوح، يمكن تحديد المسؤول عن كل جزء من العملية بسهولة. هذا التحديد يقلل من المخاطر الناتجة عن الوصول غير المصرح به، حيث يتم تطبيق تدابير تحكمية دقيقة تحد من عدد الأشخاص الذين لديهم إمكانية الوصول إلى البيانات الحساسة.					
	-64	توزيع المسؤوليات بشكل مناسب يساعد على مراقبة التعديلات التي تُجرى على البيانات وضمان توثيقها. هذا يسهم في تعزيز سلامة البيانات، حيث أن كل عملية تعديل تُراجع وتُعتمد من قبل المسؤولين المعنيين.					
	-65	وجود مسؤوليات محددة يعزز قدرة المكتبة على التعامل مع حالات الطوارئ واستعادة البيانات بسرعة. الشخص المسؤول عن النسخ الاحتياطية والتعافي من الكوارث يكون على علم تام بالإجراءات الواجب اتباعها لضمان توافر المعلومات حتى بعد وقوع حوادث سيبرانية.					
		ثـــــانيا:تكامل سياسات المكتبة مع التشريعات والمعايير العالمية للأمن السيبراني. (COBIT 5: MEA03ضمان الامتثال)؛(ISO 27001: A.18الامتثال)؛(الامتثال وإدارة المخاطرITIL)	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	-66	الامتثال للقوانين والتشريعات مثل GDPR وغيرها من المعايير العالمية يضمن تطبيق تدابير صارمة لحماية سرية البيانات الشخصية والمعلومات الحساسة، ما يقلل من فرص التسريب أو الاختراق.					
	-67	الامتثال للمعايير الأمنية يفرض على المكتبات تنفيذ تدابير الحماية التقنية مثل التشفير، التحقق متعدد العوامل، والتحديثات الأمنية الدورية، مما يحافظ على سلامة البيانات ويمنع التلاعب بها.					

-68	تتطلب التشريعات غالبًا خططًا للطوارئ واستمرارية الأعمال. الامتثال لهذه المتطلبات يضمن أن البيانات تظل متاحة حتى في حالات الانقطاع غير المخطط له.					
	ثـالثـــا:كفاءة نظام إدارة دورة حياة البيانات . (COBIT 5: DSS06 إدارة استمرارية الأعمال)؛ ISO 27001: A.8 (إدارة الأصول)	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
-69	سياسات الحفظ التي تشمل عمليات مراجعة وتدقيق دورية تساهم في الحفاظ على سلامة البيانات، حيث تتيح التعرف على أي تغييرات غير مصرح بها أو تلف قد يحدث للبيانات على المدى الطويل.					
-70	ضمان أن البيانات المطلوبة فقط هي التي تبقى محفوظة يساهم في تحسين أداء النظام، حيث يقلل من تراكم البيانات القديمة التي قد تعيق الوصول الفعّال إلى المعلومات الهامة، مما يحسن من توافر البيانات الضرورية.					
-71	تطبيق سياسات الحفظ السليمة يضمن أن البيانات التي لم تعد ضرورية يتم التعامل معها وفقًا للإجراءات المتبعة، مما يقلل من خطر تعرض البيانات غير الضرورية للاختراقات					
	رابـــــــــعا:فعالية وأمان عمليات استبعاد البيانات الحساسة. (COBIT 5: DSS06 إدارة استمرارية الأعمال) DSS02 إدارة خدمة الأمن(؛) ISO 27001: A.8 إدارة الأصول) و A.11 التحكم في الوصول(؛)ITIL إدارة الطلب والحوادث)	**موافق بشدة**	**موافق**	**محايد**	**غير موافق**	**غير موافق بشدة**
-72	إجراءات الاستبعاد المطبقة بشكل صحيح تضمن أن البيانات الحساسة لا يمكن استعادتها بعد الحذف، مما يحميها من الاستخدام غير المشروع ويضمن بقاء المعلومات الخاصة تحت السيطرة الكاملة.					
-73	تنفيذ عمليات الاستبعاد بشكل آمن يضمن عدم بقاء أي بيانات غير ضرورية قد تعرض النظام لمخاطر محتملة. تأمين عملية الحذف يمنع استخدام البيانات القديمة كمدخلات لهجمات سيبرانية.					
-74	الحذف الفعّال للبيانات غير الضرورية يساهم في تحسين الأداء العام للنظام، مما يعزز من توافر الموارد والمعلومات الضرورية بشكل أكثر كفاءة وفعالية، ويقلل من احتمالية تعطل النظام بسبب الحمولة الزائدة.					

الملحق الثالث: نتائج صدق المحكمين لأداة الدراسة

م/ب	م1	م2	م3	م4	م5	م6	م7	يقيس	لا يقيس	الفرق	الفرق/7
1	1	1	1	1	1	1	1	7	0	7	1
2	1	1	1	1	1	0	1	6	1	5	0,71
3	1	1	1	1	1	1	0	7	0	7	1
4	1	1	0	1	1	1	1	6	1	5	0,71
5	1	1	1	1	0	0	1	6	1	5	0,71
6	0	0	1	1	1	1	1	6	1	5	0,71
7	1	1	1	0	1	1	0	6	1	5	0,71
8	1	1	1	1	1	1	1	7	0	7	1
9	1	1	1	1	0	1	1	6	1	5	0,71
10	1	1	1	1	1	1	1	7	0	7	1
11	1	1	0	1	1	1	1	6	1	5	0,71

1	7	0	7	1	1	1	1	1	1	1	12
1	7	0	7	1	1	1	1	1	1	1	13
1	7	0	7	1	1	1	1	1	1	1	14
0,71	5	1	6	1	1	1	1	0	1	1	15
0,71	5	1	6	1	1	0	1	1	1	1	16
1	7	0	7	1	1	1	1	1	1	1	17
1	7	0	7	1	1	1	1	1	1	1	18
1	7	0	7	0	1	1	1	1	1	1	19
1	7	0	7	1	1	1	1	1	1	1	20
1	7	0	7	1	1	1	1	1	1	1	21
1	7	0	7	0	1	1	1	1	1	1	22
1	7	0	7	1	1	1	1	1	1	1	23
0,71	5	1	6	1	1	1	1	1	1	1	24
1	7	0	7	1	1	1	1	1	1	1	25
1	7	0	7	1	1	1	0	1	1	1	26
1	7	0	7	1	1	1	1	1	1	1	27
0,71	5	1	6	1	1	1	1	1	1	1	28
1	7	0	7	1	1	1	1	1	1	1	29
0,71	5	1	6	1	1	1	1	1	1	0	30
0,71	5	1	6	1	1	1	1	1	1	1	31
1	7	0	7	1	1	1	1	1	0	1	32
1	7	0	7	1	0	1	1	1	1	1	33
1	7	0	7	1	1	1	1	1	1	1	34
1	7	0	7	1	1	1	1	1	1	1	35
1	7	0	7	1	1	1	1	1	1	1	36
1	7	0	7	1	1	1	1	1	1	1	37
0,71	5	1	6	1	1	1	1	1	1	1	38
1	7	0	7	1	1	1	1	1	1	1	39
0,71	5	1	6	1	0	1	1	1	1	1	40
1	7	0	7	1	1	1	1	1	1	1	41
1	7	0	7	1	1	1	0	1	1	1	42

0,71	5	1	6	1	1	1	1	1	1	1	43
1	7	0	7	1	1	1	1	1	1	1	44
1	7	0	7	1	1	1	0	1	1	1	45
0,71	5	1	6	1	1	1	1	1	1	1	46
1	7	0	7	1	1	1	1	1	1	1	47
1	7	0	7	1	1	1	1	1	1	0	48
1	7	0	7	1	1	1	1	1	1	1	49
1	7	0	7	1	1	1	1	1	1	1	50
1	7	0	7	1	1	1	1	1	1	1	51
1	7	0	7	1	1	1	1	1	1	1	52
1	7	0	7	1	1	1	1	1	1	1	53
0,71	5	1	6	1	1	1	1	1	1	1	54
1	7	0	7	1	1	1	1	1	1	1	55
1	7	0	7	1	1	1	0	1	1	1	56
1	7	0	7	1	1	1	1	1	1	1	57
0,71	5	1	6	1	1	1	1	1	1	1	58
1	7	0	7	1	1	1	1	1	1	1	59
0,71	5	1	6	1	1	0	1	1	1	1	60
1	7	0	7	1	1	1	1	1	1	1	61
1	7	0	7	1	1	1	1	1	0	1	62
1	7	0	7	1	1	1	1	1	1	1	63
1	7	0	7	0	1	1	1	1	1	1	64
1	7	0	7	1	1	1	1	1	1	1	65
1	7	0	7	1	1	1	1	1	1	1	66
1	7	0	7	1	1	1	1	1	1	1	67
1	7	0	7	1	1	1	1	1	1	1	68
1	7	0	7	1	1	1	1	1	1	1	69
1	7	0	7	0	1	1	1	1	1	1	70
0,71	5	1	6	1	1	1	1	1	1	1	71
1	7	0	7	1	1	1	1	1	1	1	72
1	7	0	7	1	1	1	1	1	1	0	73

1	7	0	7	0	1	1	1	1	1	1	74

الملحق الرابع: نسبة الاتفاق بين المحكمين

	رقم الفقرة	الملاحظ الاول	الملاحظ الثاني	نقاط الاتفاق	نقاط الاختلاف
	1	✓	✓	1	0
	2	X	✓	✓	1
	3	✓	✓	1	0
	4	X	✓	✓	1
	5	✓	X	0	1
	6	✓	X	0	1
	7	✓	X	0	1
	8	✓	✓	1	0
	9	✓	X	0	1
	10	✓	✓	1	0
	11	✓	X	0	1
	12	✓	✓	1	0
	13	✓	✓	1	0
	14	✓	✓	1	0
	15	X	✓	0	1
	16	✓	X	0	1
	17	✓	✓	1	0
	18	✓	✓	1	0
	19	✓	✓	1	0
	20	✓	✓	1	0
	21	✓	✓	1	0
	22	✓	✓	1	0
	23	✓	✓	1	0
	24	✓	X	0	1

0	1	✓	✓	25	
0	1	✓	✓	26	
0	1	✓	✓	27	
1	0	✓	X	28	
0	1	✓	✓	29	
1	0	X	✓	30	
1	0	X	✓	31	
0	1	✓	✓	32	
0	1	✓	✓	33	
0	1	✓	✓	34	
0	1	✓	✓	35	
0	1	✓	✓	36	
0	1	✓	✓	37	
1	0	✓	X	38	
0	1	✓	✓	39	
1	0	X	✓	40	
0	1	✓	✓	41	
0	1	✓	✓	42	
1	0	X	✓	43	
0	1	✓	✓	44	
0	1	✓	✓	45	
1	0	✓	X	46	
0	1	✓	✓	47	
0	1	✓	✓	48	
0	1	✓	✓	49	
0	1	✓	✓	50	
0	1	✓	✓	51	
0	1	✓	✓	52	
0	1	✓	✓	53	
1	0	✓	X	54	
0	1	✓	✓	55	

0	1	✓	✓	56	
0	1	✓	✓	57	

ملخصات

ملخص باللغة العربية.

ملخص باللغة الإنجليزية

ملخصات الدراسة

ملخص

تسعى هذه الدراسة إلى استكشاف أثر تطبيق مبادئ حوكمة المعلومات على مخاطر الأمن السيبراني في بيئة المكتبات الجامعية، والتي أصبحت تعتمد بشكل متزايد على النظم الرقمية في إدارة مصادرها وخدماتها. وقد لوحظ أن تزايد التهديدات السيبرانية، مثل الاختراقات وتسريب البيانات، الأمر الذي يفرض تحديات كبيرة على المكتبات، مما يستدعي تبني أطر حوكمة فعّالة لإدارة المعلومات وحمايتها.ولقد خلصت الدراسة على مجموعة من النتائج مفادها: أن عينة الدراسة يغلب عليها الطابع الخبير، حيث يشكل الموظفون ذوو الخبرة المتوسطة إلى الطويلة النسبة الأكبر، وهو مؤشر مهم في سياق تحليل مدى إدراك العاملين بالمكتبات الجامعية لقضايا الحوكمة والمخاطر السيبرانية.وان مستوى وعي اخصائي المعلوماتلمخاطر الامن السيبراني متوسطة على مستوى مكتبات الشرق الجزائري، إضافة إلى أن اهتمام المكتبات الجامعية محل الدراسة بالرفع من مستوى وعي لدى أخصائيي المعلومات بالمفاهيم الأساسية لمخاطر الأمن السيبراني متوسط ما يعكس فهمًا مفاهيميًا وتقنيًا مقبولًا لأبعاد هذه المخاطر من حيث تأثيرها على سرية البيانات وسلامتها وتوافرها.وفي ضوء ذلك، توصي الدراسة بضرورة تعزيز سياسات الحوكمة، وتكاملها مع خطط الأمن السيبراني، وتوفير البنية التحتية والموارد التقنية والبشرية اللازمة لحماية المعلومات في المكتبات الجامعية.

الكلمات المفتاحية: حوكمة المعلومات؛ مخاطر الأمن السيبيراني؛ المكتبات الجامعية؛ الشرق الجزائري

ملخصات الدراسة

Abstract

his study aims to explore the impact of applying information governance principles on cybersecurity risks in the context of university libraries, which are increasingly relying on digital systems to manage their resources and services. The growing number of cyber threats—such as data breaches and intrusionsposes significant challenges to libraries, thereby necessitating the adoption of effective information governance frameworks to manage and protect data.

The study concluded with several findings, most notably that the sample primarily consisted of experienced professionals, with the majority of participants having moderate to extensive experience. This is a significant indicator when analyzing the level of awareness among university library staff regarding governance and cybersecurity issues. The study found that the level of awareness among information specialists regarding cybersecurity risks is moderate in university libraries located in Eastern Algeria. Moreover, the level of institutional effort to raise awareness among information specialists about the fundamental concepts of cybersecurity risks was also moderate, reflecting an acceptable conceptual and technical understanding of the risks—particularly in terms of data confidentiality, integrity, and availability.

In light of these findings, the study recommends strengthening information governance policies, integrating them with cybersecurity strategies, and providing the necessary technical infrastructure and human

Keywords: Information Governance; Cybersecurity Risks; University Libraries; Eastern Algeria