

مخاطر وتحديات أمن مصادر المعلومات بالمستودعات الرقمية للجامعات الجزائرية

Risks and Challenges of Information Security in Digital Repositories of Algerian Universities

لخضر خليلي^{1*}، عفيف غوار²¹ جامعة وهران 1 أحمد بن بلة (الجزائر)، khelili.lakhdar@edu.univ-oran1.dz² جامعة وهران 1 أحمد بن بلة (الجزائر)، ghouarafif@gmail.com

تاريخ النشر: 2025/06/01

تاريخ القبول: 2025/05/17

تاريخ الاستلام: 2024/09/05

ملخص:

يهدف هذا البحث إلى ضرورة تبني الجامعات الجزائرية إلى سياسة أمن المعلومات بالمستودعات الرقمية لما له من تعزيز ديمومة حفظ وإتاحة المصادر الرقمية على المدى البعيد ومعرفة المخاطر والتحديات في ظل تطور تقنيات المعلومات والاتصالات. توصلنا من خلال هذا البحث أن المستودعات الرقمية بالجامعات الجزائرية قد تكون عرضة لعدة مخاطر متعلقة بالانتهاك والتعدي على المعلومات وحقوق الغير في ظل الانتشار الواسع للتكنولوجيا الحديثة لذا يجب أن تكون لدى مسؤوليها ثقافة بأمن المعلومات والمخاطر التي قد تهددها ووجب عليهم صياغة سياسة واضحة ومكتوبة لمواجهة هذه المخاطر التي قد تشكل خطر على مستقبل نظام المعلومات بالمستودعات الرقمية.

كلمات مفتاحية: أمن المعلومات؛ المستودعات الرقمية؛ الوصول الحر؛ الجامعات؛ الجزائر

Abstract:

This research aims to emphasize the necessity for Algerian universities to adopt an information security policy for their digital repositories, as it plays a crucial role in ensuring the long-term preservation and accessibility of digital resources, as well as understanding the risks and challenges in light of the development of information and communication technologies.

Through this research, we have concluded that digital repositories in Algerian universities may be exposed to several risks related to information breaches and violations of others' rights due to the widespread use of modern technologies. Therefore, those responsible must have a strong awareness of information security and the risks that may threaten it. They should also develop a clear and written policy to confront these risks, which may endanger the future of the information system in digital repositories.

Keywords: Information Security; Digital Repositories; Open Access; Universities; Algeria.

*المؤلف المرسل

1. مقدمة:

إن مختلف المؤسسات وأنظمة المعلومات لديها بيانات ووثائق باختلاف وعائها وشكلها ومعلوماتها، ومع تطور شبكات الاتصالات وتكنولوجيا المعلومات الحديثة ساهمت هذه الأخيرة في إدارتها للمعلومات من خلال جمعها، معالجتها، تخزينها وإتاحتها لمتخذي القرار أو المتعاملين معها، ولقيمة المعلومة وأهميتها لنظام المعلومات يجب وضع سياسة لأمنها وحمايتها من الاستغلال غير المسموح به أو الاطلاع عليها دون إذن مالكيها، ولهذا اتجهت مختلف المؤسسات إلى تأمين معلوماتها السرية وحمايتها من الاختراق والانتهاكات أو ما يعرف بأمن المعلومات.

ومن بين المؤسسات الجامعات من خلال أنظمة المستودعات الرقمية بها التي تحتوي على مصادر معلومات رقمية ولأهميتها وحاجة المجتمع لاستخدامها والإفادة منها في جميع مجالات التنمية والتطور وجب على مسؤولي الجامعات عامة ومسؤولي المستودعات الرقمية لهذه الجامعات خاصة العمل على حمايتها وأمنها من جميع الأخطار والانتهاكات سواء كانت مقصودة أو غير مقصودة ناتجة عن سوء الاستغلال الأمثل والسليم للأنظمة بغرض حفظها على المدى البعيد وديمومتها

إشكالية الدراسة:

مع الانفجار المعرفي والتطور التكنولوجي وشبكات الاتصالات ظهر ما يسمى بمجتمع المعلومات إذ استغلته المؤسسات الاقتصادية والخدماتية في تحسين أدائها حتى ظهرت المعلومات كثروة ومورد مهم للمؤسسات إذ كرس جل مواردها للحصول عليها واستغلالها من طرف متخذي القرار وحمايتها وأمنها باعتبارها من أسرار ذكائها ويقظتها لتحقيق الميزة التنافسية ومن أجل هذا تتوجه المؤسسات نحو تطبيق معايير وإرشادات دولية وتطبيقات وأجهزة لحماية وأمن معلوماتها الاستراتيجية وتوفير إتاحتها بشكل آمن ومن بين هذه المؤسسات والأنظمة المستودعات الرقمية للجامعات الجزائرية وعليه نطرح السؤال

الرئيسي التالي:

- كيف يمكن للمستودعات الرقمية بالجامعات الجزائرية تحدي مخاطر أمن مصادر المعلومات بها؟

إذ يوجد مبرر لهذه الدراسة وهو أهمية مصادر المعلومات بالنسبة للمستودعات الرقمية بالمؤسسات الجامعية الجزائرية وواجباتها نحو أمنها وحمايتها من المخاطر التي قد تهددها والتحديات التي يجب على مديري هذه المستودعات الرقمية اتخاذها لضمان نجاعتها وديمومتها وحفظها على المدى البعيد والإفادة منها بشكل يخدم الباحثين في الحصول على المعلومات بشكل أسرع وأيسر والجامعات في مرئيتها ومواكبتها للتطورات التكنولوجية وحصر الإنتاج الفكري المنتج على مستواها والبحث العلمي من خلال النشر الأوسع للمعلومات والمعرفة وتفادي تكرار جهود الباحثين وتوضيح الرؤية للباحثين لإيجاد الفجوة العلمية والتعمق في الأبحاث.

أهمية الدراسة:

تنبع أهمية الدراسة من أهمية مصادر المعلومات الرقمية بالمستودعات الرقمية ودور هذه الأخير في إتاحتها للباحثين وتسهيل الوصول الحر للمعلومات في ظل التطور التكنولوجي وتنمية وتطوير البحث العلمي بالمؤسسات الجامعية إلا أن المصادر الرقمية عرضة في أي وقت لمخاطر قد تضر بها أو بالمستودعات الرقمية كما هناك تحديات يجب اتخاذها من طرف مديري ومسؤولي المستودعات الرقمية بالجامعات الجزائرية للتصدي لهذه المخاطر بكل أشكالها وأنواعها.

أهداف الدراسة:

تهدف الدراسة إلى:

- التعرف على أمن مصادر المعلومات، طرق، أدوات وأبعاد حمايتها
- التعريف بالمستودعات الرقمية، خصائصها، أهدافها وأهميتها كأداة للنشر العلمي في المؤسسات العلمية.

- معرفة مخاطر وتحديات أمن مصادر المعلومات بالمستودعات الرقمية للجامعات الجزائرية وأهمية تدابير وإجراءات أمن المعلومات بها

مصطلحات الدراسة:

- المعلومات: Information

وهي نتيجة معالجة البيانات، مثل النقل والاختيار والتحليل، أو نتيجة التفسير أو الاستدلال. (أحمد، 2012، صفحة 479) وتُعرف بأنها البيانات التي تمت معالجتها لتحقيق هدف محدد أو لأغراض محددة لاتخاذ قرار، كما تُعرف بأنها البيانات التي تم تحليلها أو تفسيرها أو تجميعها لتصبح ذات قيمة بحيث يمكن تداولها وتسجيلها ونشرها وتوزيعها بشكل رسمي أو غير رسمي. (شادي، 2017، صفحة 429)

- البيانات:

وهي المادة الخام الأولية التي تستخرج منها المعلومات المسجلة، مثل الرموز والأرقام والجمل والعبارات التي يمكن تغييرها أو تحليلها. وليس لها قيمة في شكلها الأصلي إلا إذا تحولت إلى معلومات مفهومة ومفيدة. (جنان، 2010، صفحة 160)

- الأمن المعلوماتي:

من الناحية الأكاديمية أمن المعلومات هو علم يبحث في إستراتيجيات ونظريات توفير الحماية لها من مخاطر وأنشطة الإعتداء عليها، ومن الناحية التقنية استخدام أدوات ووسائل وإجراءات لضمان حمايتها من الأخطار الداخلية والخارجية، ومن الناحية القانونية فإنها موضوع بحث ودراسة التدابير لحماية سرية وسلامة المحتوى مع توفير المعلومات ومحاربة كل أنشطة الإعتداء أو استغلال نظمها في ارتكاب الجريمة، وهذا هو الهدف من سن قوانين وتشريعات الحماية للمعلومات واستعمالها غير القانوني. (رمضاني، 2016، صفحة 12)

2. أمن المعلومات

1.2 أمن المعلومات Information Security:

أمن المعلومات علم يبحث في توفير حماية المعلومات من الأخطار المهددة لها والتعدي عليها، باستعمال الوسائل والأدوات الواجب توفرها لحمايتها من الأخطار الخارجية والداخلية، والبحث عن الإجراءات المعتمدة والمعايير لمنع اختراقها من طرف أشخاص غير معنيين بها عن طريق الاتصال بغية المحافظة على أصالة وصحة هذه الاتصالات. (ممدوح، 2015، صفحة 16)

2.2 طرق وأدوات لحماية المعلومات:

حماية المعلومات أمر منذ القدم، ولكن استخدم بشكل رسمي مع التطور التكنولوجي ومن مرتكزاته: (ممدوح، 2015، صفحة 41)

- أنظمة الحماية لبرامج التشغيل.
- أنظمة الحماية للتطبيقات والبرامج.
- أنظمة الحماية لقواعد البيانات.
- حماية الولوج إلى الأنظمة.
- تأمين الأجهزة والمعدات.
- تثبيت مضاد فيروسات فعال.
- تثبيت برامج لكشف الاختراق.
- تركيب أنظمة لمراقبة الشبكة للكشف عن نقاط الضعف التأمينية.
- عمل النسخ الاحتياطي.
- تفعيل أنظمة قوية لتشفير المعلومات.
- دعم أجهزة عدم انقطاع التيار.
- نشر الوعي الأمني وتعليم الأفراد.

3.2 أهمية أمن المعلومات:

تتمثل أهمية أمن المعلومات فيما يلي: (قدايفة، 2016، صفحة 165)

1. تعتمد عليها القطاعات الاقتصادية في دقتها وصحتها.
2. الدول بحاجة لتدابير أمنية لمواجهة المخاطر التي تظهر فجأة خلال التعامل مع الأطراف الأخرى.
3. القطاع العام والخاص بحاجة إلى بيئة إلكترونية آمنة.
4. استخدام البرمجيات الإلكترونية واستعمالها بكثرة لهذا تحتاج بيئة آمنة.
5. للاستمرار في الأعمال التجارية تزداد الحاجة إلى مزيد من حماية بنية الشبكة العنكبوتية.
6. وفرة فرص الإجرام الإلكتروني بالتوازي مع تطور التقنية وازدهارها.

4.2 عناصر أمن المعلومات:

يعتمد أمن المعلومات على أربع عناصر وهي: (صالح ع.، 2018، صفحة 53)

1. العمليات: وتعتبر جوهرية لأي نظام أمني، كما تطبق بطريقة منتظمة وتراجع بانتظام من أجل استبعاد المخاطر والأخطاء.
2. الموارد البشرية: إذ ينجزون أعمالهم وخدماتهم، كما يجب توفرهم بأعداد كافية وتخصصات وخبرة مهنية ومهارة مناسبة.
3. التقنية: إذ تحتاج إلى توافر منتجين وموردين وكذلك باعين وموزعين، مما يسهل عليهم الاندماج في شركات لتفادي الخسارة والخروج من سوق الأعمال، ويصعب تقييم التقنية كما كانت سابقا.
4. الثقافة: وهي مرتبطة ببيئة الأعمال وأخلاقيات المنظمة نحو المجتمع، حيث تؤدي المنظمة دورها الرئيسي في الحفاظ على الثقافة التي تتماشى مع ثقافة المجتمع.

5.2 أبعاد حماية المعلومات:

يجب ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها:

(دلال و بن ديلي، 2020، صفحة 131).

- السرية أو الموثوقية Confidentiality: وهي التأكد من عدم كشف المعلومات وبأن لا يطلع عليها إلا المخولين بها فقط.
- سلامة المحتوى Integrity: التأكد من صحة محتوى المعلومات، وأنه لم يعدل أو تم العبث به أو تغييره خلال مراحل المعالجة أو أثناء تبادله الداخلي أو تدخل خارجي غير مشروع.
- استمرارية توفر المعلومات Availability: التأكد من عمل النظام المعلوماتي باستمرار وقدرته على التعامل مع المعلومات وتقديم المزيد من الخدمات لمواقع المعلوماتية وأنها لن تتعرض إلى منع استخدامها أو دخوله لها.
- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non- repudiation: ويقصد به نفي إنكار الشخص الذي قام بعمل متصل بالمعلومات أو المواقع، وذلك من خلال القدرة على إثبات التصرف ومن قام به ومتى قام به.

6.2 سياسة أمن المعلومات: IS Policy

هي ناتج المزج بين المبادئ والأنظمة والمنهجيات والتقنيات والأدوات المنشأة لحماية المنظمة من التهديدات، كما تعتبر وثيقة استراتيجية مكونة من الاتجاهات والأهداف والقواعد التي يجب اتباعها من طرف الموظفين المتعاملين مع المنظمة، ولهذا يجب وضوح سياسة أمن المعلومات كما يجب أن تكون شاملة وتغطي مستلزمات أمن المعلومات والتناسق مع رؤية وسياسة المنظمة. (صالح ر، 2020، صفحة 112).

3. المستودعات الرقمية

1.3 تعريف المستودعات الرقمية:

هناك عدة تعريفات للمستودعات الرقمية:

منهم من عرفها بأنها قاعدة بيانات على شبكة الأنترنت تحتوي على المصادر العلمية إذ تمتاز المستودعات الرقمية بالتراكمية والإتاحة الدائمة وهي مفتوحة وتقبل التشغيل المتبادل وجمع وتخزين ونشر المصادر وتعتبر جزء من عملية الاتصال إذ تقوم بحفظ المصادر الرقمية على المدى البعيد لأنها وظيفة أساسية للمستودعات المؤسسية، كما يعرف المستودع الرقمي بأنه مجموعة من الخدمات تقدمها المؤسسات الجامعية للمجتمع الأكاديمي لغرض إدارة ونشر المصادر الرقمية المنتجة على مستوى المؤسسة وأعضاء مجتمع البحث، ويكون هناك التزام تنظيمي للإشراف على المواد والمصادر الرقمية منها الحفظ طويل المدى والتنظيم والإتاحة أو التوزيع. (بونيف، 2021، صفحة 463)

2.3 نشأة المستودعات الرقمية:

يرجع الفضل في ظهور المستودعات الرقمية إلى مبادرات أقيمت من أجل وضع نتائج البحوث العلمية في تصرف أكبر عدد من الباحثين والوصول الحر لها دون قيود أو شروط سواء مادية أو قانونية، إذ بدأت المستودعات الرقمية في أخذ مكانة أكبر في مجال نشر وتداول البحوث العلمية في الفترة الممتدة ما بين سنة 1990 وسنة 2000 حيث عرفت هذه الفترة بحركة الأرشفات المفتوحة إذ تم إنشاء أول أرشيف مفتوح ثم بعد أرشيف للعلوم المعرفية سنة 1995 وظهرت هذه الحركات للحد من ارتفاع أسعار الدوريات العلمية إذ عجزت المكتبات الاشتراك في كامل أعدادها وتراجع البحث العلمي، فمكنت هذه الحركات من إيجاد حل بديل لتحقيق الاتصال العلمي بين الباحثين وإتاحة البحوث العلمية والمنشورات دون وساطة الناشرين التجاريين وهذا يعرف بالوصول الحر، إذ جعلها تحظى بتأييد واسع على المستوى العالمي من خلال ظهور مبادرات الوصول الحر كمبادرة بودابست ونداء باديسا ومبادرة برلين، ووسعت حيز المساهمات إلى التراث الثقافي والأبحاث الممولة من الأموال العامة

وهذا كله مهد لظهور المستودعات المؤسسية. (شورار و بن السبي، 2022، الصفحات 963 - 964)

ومن خلال ما تطرق إليه الباحث بأن المستودعات الرقمية ظهرت في نهاية القرن 20 وبداية القرن 21 وهذه الفترة بذات صاحبها تطور تكنولوجيا المعلومات والاتصال الحديثة أي انتشار الأنترنت بشكل كبير بين مختلف الدول إذ يكون للتكنولوجيا الحديثة والأنترنت الدور الأساسي في ظهور المستودعات الرقمية كأداة من أدوات الوصول الحر دون قيود قانونية أو مالية وكان لمبادرات الوصول الحر دورها في رسم الطريق نحو إتاحة البحوث العلمية والمنشورات من دون وساطة للنashرين التجاريين.

3.3 أنواع المستودعات الرقمية:

هناك أنواع متعددة للمستودعات الرقمية نذكر منها ما يلي: (لزامي و شباب، 2022،

الصفحات 03 - 04)

- المستودعات المؤسسية: إذ تكون تابعة للمؤسسات الجامعية، المعاهد ومنظمات البحث والتعليم، إذ تعمل هذه المستودعات على استيعاب واستقطاب الإنتاج الفكري للباحثين المنتسبين لهذه المؤسسات وفق سياسة يحددها مسؤولو المستودع.
- المستودعات المتخصصة أو الموضوعية: وهي التي تختص بمجال علمي محدد أو في عدة مجالات علمية ويتم إيداع البحوث والمنشورات فيها من قبل مختلف الباحثين بشكل إرادي وتطوعي من جميع المؤسسات البحثية.
- المستودعات وفقا لنوع المحتوى: تكون هذه المستودعات إما لمقالات الدوريات أو الكتب أو الرسائل الجامعية أو المؤتمرات وغيرها من المجالات المحددة النوع.
- مستودعات حسب مجال المادة: إذ تشمل تقنيات التعليم وعلم الأحياء والرياضيات والفيزياء ضف إلى ذلك علم الاجتماعيات والعلوم الأخرى.

4.3 أهداف المستودعات الرقمية:

للمستودعات الرقمية عدة أهداف متنوعة تنشأ لأجلها نوجزها فيما يلي: (بن حرية

و شاشة، 2022، الصفحات 78 - 79)

- الحد من تكاليف النشر والطباعة والمساهمة في تحقيق مجتمع المعلومات اللاورقي.
- المساهمة في تعزيز التدريس والبحث العلمي من خلال تيسير متابعة المحاضرين لأداء طلابهم وإتاحة الفرصة لهم للتركيز على الارتقاء بالعملية التعليمية.
- المساهمة في إنتاج المعرفة وتوزيع ونشر المعلومات للمجتمع بطريقة أسرع وتكلفة أقل.
- تحقيق سبل التعاون بين مؤسسات البحث العلمي والمؤسسات التعليمية والتجارية.
- الإتاحة الرقمية للمعلومات التي تفتتها المؤسسات وتمثيل نشاطها عالميا.
- حفظ مصادر المعلومات النادرة والقابلة للتلف على المدى البعيد وإتاحة الإفادة منها.
- توفير مداخل متعددة للبحث عن المعلومات ومصادرها.

5.3 مبادئ المستودعات الرقمية:

تلتزم المستودعات الرقمية بالمبادئ التالية: (Al Shobaki, Abusharekh, Abu-

Naser, & El Talla, 2020, p. 121)

- دعم المحتوى الرقمي وتشجيع إنشاء وحفظ نتائج الأبحاث.
- دعم واكتشاف نتائج الأبحاث ذات الصلة عبر المجموعات والتخصصات.
- دعم وتشجيع التعاون الوطني والدولي لتعزيز التوافقية وإدارة المحتوى الرقمي.
- دعم وتعزيز الروابط بين البحث الرقمي وخدمات التعلم والإدارة.
- دعم وتعزيز استخدام المعايير المفتوحة ذات الصلة مثل مبادرة الأرشيفات المفتوحة.
- دعم وتعزيز العمليات التي تسهل على المؤلفين والباحثين إيداع نتائج أبحاثهم.
- دعم وتعزيز الخيارات المتاحة لحفظ الكيانات الرقمية على المدى البعيد والوصول إلى المحتوى الرقمي.

6.3 أهمية المستودعات الرقمية كأداة للنشر العلمي في المؤسسات العلمية:

المستودعات الرقمية والمؤسسية تتمتع بمكانة فريدة في مؤسسات البحث العلمي، إذ تهتم بجمع وتنظيم وتوفير الوصول إلى مجموعة واسعة من مصادر المعلومات التي لا يمكن الوصول إليها وتساهم كذلك في تطوير الاتصال العلمي بين الباحثين إضافة إلى تقديم قيمة مضافة تساعد على: (بن الطيب و بيوض، 2022، صفحة 204)

- تحقيق أكبر قدر من الروابط بين محتويات المستودعات الرقمية والمنشورات العلمية.
- تسهيل البحث والاسترجاع لمختلف مصادر المعلومات الإلكترونية.
- تعزيز النشر العلمي من خلال مقالات ما قبل النشر، أشكال رقمية مختلفة
- تحرير الاتصال العلمي ودفعه بما يتماشى واحتياجات البحث العلمي.
- حصاد الأبحاث العلمية والحصول على مجموعة واسعة من المواد الرقمية وتعزيز المرئية المهنية للباحثين.
- تعتبر المستودعات الرقمية أداة ذات قيمة لمتابعة الإنتاج الفكري بالجامعة ومرآة عاكسة للبحث العلمي ومنه إمكانية التعرف على القيمة العلمية للمؤسسة.
- تعد المستودعات أداة مهمة تمكن من إدارة الخبرات وإبرازها والمساهمة في تقييم البحوث وتثمينها.
- تحقيق مرئية عالمية لنتائج البحوث وبث الإنتاج العلمي للجامعة.
- تحقيق الحفظ على المدى البعيد وبشكل آمن للإرث العلمي للمؤسسة، بالإضافة إلى إمكانية الاسترجاع والاستعمال السهل للوثائق العلمية المخزنة بها.
- أداة للاتصال العلمي المباشر من أجل خدمة سياسة المؤسسة العلمية فهي تساهم في نشر وإعطاء قيمة مضافة لنتائج البحوث العلمية.

4. مخاطر وتحديات أمن مصادر المعلومات بالمستودعات الرقمية للجامعات الجزائرية

1.4 المستودعات الرقمية بالجامعات الجزائرية:

من خلال الاطلاع وتصفح الموقع الرسمي لوزارة التعليم العالي والبحث العلمي الجزائرية بتاريخ 29 جانفي 2024 قمنا بإحصاء المؤسسات الجامعية بما فيها الجامعات والمراكز الجامعية فقط إذ تم إحصاء ناحية الشرق 24 مؤسسة جامعية منها 02 فقط مراكز جامعية وناحية الوسط بها 20 مؤسسة جامعية منها 03 مراكز جامعية أما ناحية الغرب بها 19 مؤسسة جامعية منها 04 مراكز جامعية وهذا كله ما مجموعه 63 مؤسسة جامعية ولكن المستودعات الرقمية من خلال الاطلاع على مواقعها وتصفحها أحصينا 43 مستودع رقمي وهو ما يعادل 68.25 % من مجموع الجامعات زائد المراكز الجامعية وهذا العدد معتبر يمكنه استيعاب مصادر المعلومات الرقمية بمختلف أنواعها وإتاحتها عبر شبكة الأنترنت للباحثين بأسرع وأيسر الطرق وهذا ما ينعكس بالإيجاب على ترقية البحث العلمي ومرئية الجامعة والتعريف بالباحثين والاستفادة من البحوث السابقة وتفادي تكرار الجهود إلا أن مديري المستودعات الرقمية أمامهم تحدي كبير وهو أمن المعلومات الرقمية بالمستودعات الرقمية من كل الأشكال المنافية والمضرة بأنظمة المعلومات والحقوق الفكرية لمالكها.

2.4 أهمية تدابير وإجراءات أمن المعلومات بالمستودعات الرقمية:

هناك العديد من الأخطار التي تواجه مصادر المعلومات الرقمية بالمستودعات الرقمية والتي لا بد من أخذها بعين الاعتبار قبل الشروع في بناء أي مستودع رقمي لأي جامعة وعلى الجامعات الجزائرية وضعها ضمن سياسة حماية المستودعات الرقمية من هذه المخاطر التي منها نذكر الاختراقات الإلكترونية، البرمجيات الخبيثة، الخصوصية وحماية البيانات، التحديثات الأمنية، إدارة الوصول والصلاحيات، التوعية والتدريب حول أمن المعلومات، البنية التحتية الضعيفة والنسخ الاحتياطي كإجراء لأمن المعلومات كل هذه التحديات يجب على مديري المستودعات الرقمية وضع استراتيجية للتصدي لهذه المخاطر والتحديات قصد

ضمان أمن المعلومات الرقمية بالمستودعات إذ توجد تدابير وإجراءات لأمن المعلومات ضد هذه المخاطر تساعد في: (صغير، 2015، الصفحات 76 - 77)

- أ. حفظ الإنتاج الفكري وحمايته من أشكال الجريمة الإلكترونية.
- ب. إتاحة البحوث العلمية وتداولها من خلال عملية البث والنشر دون تحريف أو تحوير.
- ت. حماية الملكية الفكرية للمبدعين والباحثين.
- ث. احترام خصوصية الإنتاج الفكري وعدم التعدي عليه وسن قوانين وتشريعات لحماية الحقوق والحريات والخصوصية.

3.4 مخاطر وتحديات أمن المعلومات بالمستودعات الرقمية:

توجد العديد من المخاطر التي تواجه أمن المعلومات بصفة عامة وأمن المستودعات الرقمية للمؤسسات الجامعية بصفة خاصة والتي يجب على مديري المستودعات الرقمية الاحتياط ومحاولة التصدي لهذه المخاطر التي تهدد أمن مصادر المعلومات الرقمية والبيانات ونذكر من بين هذه المخاطر ما يلي:

1.3.4 الاختراق:

هو القدرة على الوصول للهدف والدخول على الأجهزة بطريقة غير قانونية لهدف التطفل وإلحاق الضرر بهم من خلال ثغرات في نظام الحماية الخاص بها ويسمى المخترق بـ "هاكر" وعندما يتمكن هذا الأخير من إحداث أضرار كحذف ملفات أو زرع ملفات تجسسية أو فيروسات يعتبر مخرب، ويتم الاختراق من خلال معرفة الثغرات الموجودة في النظام والتي تكون غالباً في المنافذ الخاصة بالأجهزة ويمكن وصف هذه المنافذ بأنه بوابات الأجهزة على شبكة الأنترنت. (الحمداني، 2013، صفحة 13)

ومن خلال ما سبق يجب على مديري المستودعات الرقمية العمل على اكتشاف الثغرات الموجودة في النظام كأن يقوم بمحاولة تجريبية لاختراق المستودع لاكتشاف الثغرة التي تكون بنظام المستودع الرقمي وتكون محتملة للمخترقين اكتشافها وسدها وتقليل نسبة مخاطر الاختراق من جهات خارجية وإحداث أضرار بالمستودع.

2.3.4 البرمجيات الخبيثة:

هي البرامج التي تكون كل مهامها أو أحدها خبيث مثل التجسس أو التخريب ودوافع تطوير هذه البرمجيات الخبيثة هي إثبات الشخص أنه قادر على تطوير برمجيات تستطيع الاختراق أو التجسس أو التخريب وسرقة المعلومات لغرض الحصول على معلومات سرية بالمؤسسة المنافسة أو لدولة ما أو الانتقام من الأفراد والمؤسسات والدول. (القحطاني و الغنير، 2009، صفحة 58)

ويعرف كذلك بأنه مصطلح عام لجميع أنواع البرمجيات الضارة في سياق أمن أجهزة الكمبيوتر وتستخدم هذه البرمجيات بهدف محاولة اختراق سياسة أمن نظام الكمبيوتر فيما يتعلق بالسرية أو النزاهة أو التوافر. (Sharp, 2007, p. 01)

ولهذا وجب على المؤسسات الجامعية توفير أنظمة حماية الأنظمة تكون قوية لمديري المستودعات الرقمية وتحديثها باستمرار لضمان نجاعتها وفعاليتها وبقاء مديري المستودعات الرقمية في وضعية احترازية لأي اختراق أو برمجية خبيثة لضمان أمن المعلومات الرقمية بنسبة كبيرة.

3.3.4 التخزين السحابي أو الحوسبة السحابية:

في الحوسبة السحابية أو التخزين السحابي يمكن مشاركة البيانات عن طريق شبكة الأنترنت من أي مكان وأي وقت عبر أي جهاز إلكتروني ويمثل بديلا لطرق التخزين التقليدية المحدودة في الحجم والسرعة والوصول إلى البيانات والمعلومات وتعرف الحوسبة السحابية حسب المعهد الوطني للمعايير التقنية بأنها نموذج هدفه تمكين الوصول إلى الشبكة الحاسوبية بشكل مريح ومن أي مكان بناء على طلب المستفيد حيث يوجد تجمع مشترك لموارد حاسوبية كالشبكات والخوادم والتطبيقات والخدمات الإلكترونية وأماكن التخزين التي يمكن توفيرها ونشرها بأقل جهد إداري ممكن وبدون تدخل من مزودي الخدمة. (آل حيان، 2019، صفحة 43)

ويشير التخزين السحابي إلى مساحة تخزين افتراضية يمكن أن تمتد عبر العديد من أجهزة التخزين المادية المختلفة، وعندما يستخدم التخزين السحابي قد تكون بعض الملفات على خادم في نيويورك بينما تكون ملفات أخرى على خادم آخر في كاليفورنيا ونظرا لأن معظم المستخدمين لا يعرفون أين توجد ملفاتهم المادية، ويمكن اعتبار استخدام التخزين السحابي شيئا غامضا وغير ملموس مثل السحابة نفسها. (Community Workshop Serier, 2015, p. 03)

وبما أن التخزين السحابي يمكن من مشاركة البيانات عبر شبكة الأنترنت ومن أي مكان باستخدام أجهزة إلكترونية فهي عرضة كذلك للاختراق والقرصنة والتجسس والتعدي على البيانات الموجودة بنظام المستودع الرقمي لذا يجب الاحتياط لمثل استغلال هذا التخزين والاعتماد على التدابير الأمنية لحماية المعلومات الرقمية.

4.3.4 الخصوصية وحماية البيانات:

اعترفت العديد من الدول والتشريعات بالحق في الخصوصية إلا أن حماية هذه الخصوصية تبقى عرضة للاعتداءات والانتهاكات ليس لنقص التشريعات التي تنظم هذه الممارسات وإنما لتطور التقنيات في مجال المعلومات والاتصالات التي لا يمكن توقع إمكاناتها ونتائجها مثل تقنيات رصد وجمع البيانات وتتبعها ومعالجتها والتنقيب عليها والوصول إليها بسرعة فائقة من طرف أكبر عدد من المستخدمين في أماكن متعددة من العالم، زيادة على ذلك يستحيل معالجة النتائج السلبية للاعتداءات على المعلومات والبيانات في كثير من الأحيان ويصعب استعادة البيانات التي تم التعدي عليها أو تعذر سحب البيانات التي تم نشرها أو تشويهها وتزويرها والتلاعب بها كما لا ننسى خطر اقتحام قواعد المعلومات الشخصية للمؤسسات أو الجهات الرسمية. (جبور، د.ت.، الصفحات 120 - 121)

ومنه يجب حماية البيانات الشخصية بالمستودعات الرقمية وتفاذي نشر الأخبار والبيانات المزورة وتشويه المعلومات.

5.3.4 إدارة الوصول والصلاحيات:

الهدف من نظام التحكم في الوصول يجعل السياسات الأمنية تعكس العمليات الفعلية للمؤسسة وكل فرد في المنظمة أو الإدارة يمنح فقط الأدوار الضرورية لإتمام عمله بنجاح وكل دور يحتوي على الإذن اللازم لأداء المهام المخولة والمحددة وبما أن نظام التحكم في الوصول الذي يعتمد على الدور يرتبط مباشرة بوظائف الأفراد الحقيقية ومنه يستطيع مسؤولو أمن المعلومات العمل مع مستخدمي النظام وذلك بهدف تطوير وتطبيق السياسة الخاصة بأمن المعلومات هذا أمر مهم لمستخدمي النظام باعتبارهم خبراء في هذا الموضوع ويعرفون أذونات النظام اللازمة لوظيفة معينة والمهام المرتبطة بها. (أغروال، كامبو، بيرس، و العلوان، 2018، صفحة 405)

ومن خلال ما سبق يجب على كل فرد ضمن نظام معلومات المستودع الرقمي القيام بالدور المنوط به فقط لأداء مهامه المحددة وهم من يعرفون الأذونات اللازمة لأي وظيفة ولهذا مديري المستودعات الرقمية أمام تحدي آخر وهو إدارة الوصول والصلاحيات لكل موظف ومستخدمي النظام ضمن الصلاحيات المخولة لهم.

6.3.4 التحديثات الأمنية:

وتعتبر التحديثات الأمنية بمثابة إصدار جديد لتصحيح ثغرة أمنية معينة تم اكتشافها في النظام، معناه إذا لم تصلح فإنه يتم استغلالها للإخلال بأمن معلومات النظام أو المخزنة في الجهاز الذي يعمل عليه النظام (القحطاني و الغثير، 2009، صفحة 104) وعليه فإن التحديثات الأمنية وتصحيح الثغرات الموجودة التي تم اكتشافها في النظام تبقى ضرورية لتفادي استغلالها في اختراق نظام المستودع الرقمي

7.3.4 النسخ الاحتياطي كإجراء لأمن المعلومات:

تتعطل الأنظمة وأجهزة الكمبيوتر بشكل مفاجئ مما يعرض التسجيلات الحيوية للنظم ومنتجات العمل إلى فقدان بدون رجعة خاصة إذا تم تخزين المعلومات والبيانات على تلك الأجهزة فقط، وقد يتسبب فقدان البيانات إلى زيادة تكلفة العمل، لذا يجب النسخ

الاحتياطي للبيانات من أجل استعادتها عند الضرورة ومن أهداف النسخ الاحتياطي توفير تخزين آمن لأصول البيانات ومنع فقدانها في حالة الحذف أو تلفها أو فشل النظام أو حدوث كوارث سواء طبيعية أو بشرية والسماح باستعادة البيانات المؤرشفة في الوقت المناسب. (الهيئة الوطنية لأمن وسلامة المعلومات، د.ت.، صفحة 106)

من خلال ما سبق ذكره يجب على مسؤولي ومديري المستودعات الرقمية بالجامعات الجزائرية النسخ الاحتياطي لبيانات ومعلومات المستودعات الرقمية حفاظا على ديمومة النظام وأمنه من الأخطار التي تهدده أو الفشل المفاجئ للأنظمة أو حدوث الكوارث لأن الدول تعيش حاليا تقلبات جوية قد تؤول إلى كارثة طبيعية وأزمات سياسية واقتصادية ونزاعات أدت معظمها إلى حروب مدمرة تكون خطر على المنشآت الحيوية والبنى التحتية للدول المتنازعة ولهذا النسخ الاحتياطي للأنظمة المعلومات ومن الأفضل يكون في غرف محصنة من كل أنواع المخاطر للحفاظ على ديمومة النظام والمؤسسة.

5. خاتمة:

للمستودعات الرقمية بالجامعات دور مهم في جمع وحفظ وإتاحة مصادر المعلومات على المدى البعيد وإثراء البحث العلمي وحفظ التراث الفكري للجامعات إذ انتشرت هذه المستودعات في ظل التطور التكنولوجي والتقنيات الحديثة للاتصال ولا يمكن لهذه المستودعات أن تستمر وتؤدي ما هو مطلوب منها دون أن تأخذ على عاتقها أمن مصادر المعلومات الرقمية بها إذ تعد حلقة مهمة في نظام المعلومات لذا وجب على مسؤولي المستودعات الرقمية بالجامعات الجزائرية الوعي بأهمية المعلومات وحمايتها من جميع المخاطر التي قد تؤدي إلى انتهاكها وتشويهها وتحريفها أو اتلافها وقد تلخصت نتائج الدراسة أن تحديات أمن مصادر المعلومات بالمستودعات الرقمية هي:

- وجوب حماية نظام المعلومات للمستودعات الرقمية من كل أشكال الاختراق وسد الثغرات الأمنية بها.

- محاربة البرمجيات الخبيثة من خلال تثبيت مضادات لها وتحديثها باستمرار حفاظا على نظام المعلومات بالمستودعات الرقمية مهما كلف الثمن.
- التعامل بحذر من التخزين السحابي لمصادر المعلومات بالمستودعات الرقمية قد تكون عرضة للاختراق والتلف أو القرصنة.
- حماية البيانات الشخصية وتفادي نشر المعلومات المزورة والمشوهة.
- التحكم في إدارة وصول الأفراد العاملين والمستخدمين للمستودعات الرقمية ضمن إطار المهام والأذونات المحددة لأداء المهام أو الوصول للمعلومة فقط من طرف المستخدمين.
- التحديث الدوري لنظام المعلومات قصد تصحيح الثغرات الأمنية التي تم اكتشافها من قبل منتج برمجية النظام لتفادي الاختراق بنسبة أقل.
- النسخ الاحتياطي لنظام المعلومات حفاظا على ديمومته في حالة وقوع كوارث طبيعية أو بشرية لتقليل من تكلفة العمل والبدء من جديد.
- سن المزيد من التشريعات في مجال محاربة الجريمة الإلكترونية واختراق أنظمة المعلومات.
- الانضمام إلى الهيئات الوطنية والدولية لمكافحة الجريمة الإلكترونية واختراق الأنظمة.
- تنظيم والمشاركة في الملتقيات الوطنية والدولية وندوات التوعية بخطورة انتهاك مصادر المعلومات واعلام الرأي العام بعقوبة الانتهاكات لكبح نوايا المخترقين الهواة.

6. قائمة المراجع:

- Al Shobaki, M., Abusharekh, N., Abu-Naser, S., & El Talla, S. (2020, August). The Reality of Using Digital Repositories at the University of Palestine. *International Journal of Academic Accounting, Finance & Management Research (IJAAFMR)*, 04(08).
- Community Workshop Serier. (2015, December). INTRODUCTION TO CLOUD STORAGE. Retrieved from cws.web.unc.edu
- Sharp, R. (2007). An Introduction to Malware.
- الهيئة الوطنية لأمن وسلامة المعلومات. (د.ت.). *السياسات الوطنية لأمن وسلامة المعلومات*. ليبيا.

- أمينة قدايفة. (2016). إستراتيجية أمن المعلومات. *مجلة أعداد إقتصادية* (06).
- بشرى حسين الحمداني. (2013). *القرصنة الإلكترونية أسلحة الحرب الحديثة*. عمان: دار أسامة للنشر والتوزيع.
- خالد بن ناصر آل حيان. (2019). *الحوسبة السحابية أساسيات ومبادئ وتطبيقات*. المملكة العربية السعودية، معهد الإدارة العامة: مركز البحوث والدراسات.
- خولة شادي. (2017). *المعلومات وصنع القرار عبر اليقظة الإستراتيجية: نحو نظام فعال لسيرورة المعلومات*. *مجلة العلوم الإجتماعية والإنسانية* (12).
- رضا إبراهيم صالح. (2020). دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية مع دراسة ميدانية على الشركات المصرية. *مجلة الدراسات التجارية المعاصرة*، 06(10).
- زينب بن الطيب، و نوجود بيوض. (26 جانفي، 2022). دور أخصائي المعلومات في تفعيل توجهات المكتبات الجامعية لتحفيز الباحثين نحو دعم المستودعات المؤسسية كآلية للنشر: دراسة ميدانية. *مجلة هيروودوت للعلوم الإنسانية والإجتماعية*، 06(01).
- صادق عبد الرزاق جنان. (2010). تأثير تكنولوجيا المعلومات في إدارة المعلومات والمعرفة. *مجلة كلية التربية الأساسية/ جامعة بابل* (03).
- عفيفة شورار، و عبد المالك بن السبي. (15 مارس، 2022). الإنتاج الفكري الجامعي وتحديات المكتبات الجامعية في التعريف به من خلال المستودعات الرقمية المؤسسية: دراسة ميدانية بالمكتبة المركزية لجامعة الحاج لخضر باتنة1. *مجلة المعيار*، 26(64).
- علي أحمد. (2012). مفهوم المعلومات وإدارة المعرفة. *مجلة جامعة دمشق*، 28(01).
- علي محمود ممدوح. (كانون الأول، 2015). استخدامات التخزين السحابي للبيانات في المكتبات ومراكز المعلومات وأمن المعلومات. *المجلة الأردنية للمكتبات والمعلومات*، 50(04).
- عوض الله أحمد حسين صالح. (2018). أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعات الأردنية. أطروحة دكتوراه *فلسفة في نظم المعلومات الإدارية*. جامعة السودان، السودان.
- فاطمة صغبر. (2015). دور الأمن المعلومات في حماية البحوث والدراسات العلمية. *الملتقى الوطني حول: الأمن المعلوماتي: مبادئه وسبل الحماية*. تيزي وزو.

- قوقو لزامي، و فاطمة شباب. (13 نوفمبر، 2022). إستراتيجية إعداد المستودعات الرقمية المؤسساتية ودورها في دعم الوصول الحر : المدرسة الوطنية العليا للسياسة بالحراش الجزائر أنموذجا. مجلة علم المكتبات، 14 (01).
- كمال رمضان. (2016). الأرشيف بين التوثيق والأمن المعلوماتي. الملتقى الوطني حول الأمن المعلوماتي: مبادئه وسبل الحماية. تيزي وزو.
- لخضر دلال، و اسماعيل بن ديلي. (05، 04، 2020). المورد البشري خطر أم حصن للمنظمة؟ مدخل: أمن المعلومات في ظل الذكاء الإقتصادي. مجلة الأفاق للدراسات الإقتصادية، 05 (01).
- مانيش أغروال، أليكس كامبو، إيرك بيرس، و جعفر بن أحمد العلوان. (2018). أمن المعلومات وإدارة مخاطر تقنية المعلومات. المملكة العربية السعودية، معهد الإدارة العامة: مكتبة الملك فهد الوطنية.
- محمد بن عبد الله القحطاني، و خالد بن سلمان الغنبر. (2009). أمن المعلومات بلغة ميسرة. الرياض: مكتبة الملك فهد الوطنية.
- محمد لمن بونيف. (ديسمبر، 2021). دور المستودعات الرقمية المؤسساتية في إتاحة الأدب الرمادي الجزائري من وجهة نظر أساتذة كلية العلوم الانسانية والاجتماعية بجامعة المسيلة. حوليات جامعة الجزائر 1، 35 (04).
- منى الأشقر جبور. (د.ت.). السيرانية: هاجس العصر. (جامعة الدول العربية، المحرر)
- نجاة بن حريرة، و فارس شاشة. (04 ديسمبر، 2022). الوصول الحر للأدب الرمادي بالمستودعات الرقمية الأكاديمية الجزائرية: مستودع جامعة بسكرة نموذجا. مجلة المقدمة للدراسات الإنسانية والاجتماعية، 07 (02).