مجلة الامتياز لبحوث الاقتصاد والإدارة
ISSN 2572-0171
المجلد 10، العـدد: 01 (2026)،
ص 286- 302

Journal of Excellence for Economics and Management Research
ISSN 2572-0171
Vol 10, N°01 : (2026)
P 286.-302

فعالية المرونة السيبرانية في حماية البيانات الأكاديمية للمؤسسات الجامعية في الجزائر

محمد يدو [1] (*)، فتيحة بارة [2]

[1] دكتوراه، أستاذ التعليم العالي (جامعة البليدة -2-)، (الجزائر)
yedou_m@yahoo.fr
[2] دكتوراه، (جامعة البليدة -2-)، (الجزائر)
https://orcid.org/0009-0001-7744-8474
fellafatiha.bara@gmail.com
https://orcid.org/0009-0001-7744-8474

تاريخ الاستلام: 2025-10-21 **تاريخ القبول:** 2026-05-19 **تاريخ النشر:** 2026-06-05

ملخص: تهدف هذه الدراسة إلى التعرف على أهمية وجود بيئة رقمية تتميز بالمرونة السيبرانية في حماية البيانات الأكاديمية للمؤسسات الجامعية التي تنشر على مواقع الويب، في ظل زيادة التهديدات والتحديات الأمنية كالقرصنة والاختراقات السيبريانية وغيرها.

ولتحقيق أهداف الدراسة تم الاعتماد على المنهج الوصفي التحليلي لمعالجة الإشكالية، فتوصلنا إلى أن المرونة السيبرانية توفر إطار عمل متكامل يتضمن صياغة استراتيجيات في مجال الأمن السيبراني لتقييم المخاطر السيبرانية والكشف عنها بشكل مبكر والاستجابة لها واستعادة النشاط في حال حدوث اختراق للبيانات، كما يجب وضع سياسات وبرامج البحث والتطوير والابتكار لبناء مستوى عالي لأمن البنى الأساسية لتكنولوجيا المعلومات والشبكات الذي يفي بمعايير الأمان في حماية البيانات الأكاديمية بالجامعات الجزائرية.

الكلمات المفتاحية: مرونة سيبرانية، حماية، بيانات أكاديمية، الجامعات الجزائرية.

تصنيف JEL: L86 ,K24 ,C80,I23

(*) المؤلف المرسل

المعرف الرقمي للمقال (doi): https://doi.org/10.34118/jeemr.v10i1.4597

Journal of Excellence for Economics and Management Research
ISSN 2572-0171
Vol 10, N°01 : (2026)
P 286.-302

مجلة الامتياز لبحوث الاقتصاد والإدارة
ISSN 2572-0171
المجلد 10، العـدد: 01 (2026)،
ص 286- 302

The effectiveness of cyber resilience in protecting academic data of university institutions in Algeria

1st Mohamed yedou [1(*)], 2nd Fatiha bara [2]

[1] Doctorat, professor, Affiliation (University Blida 2.) (Algeria)
✉fellafatiha.bara@gmail.com
https://orcid.org/0009-0001-7744-8474

[2] Doctorat, (University Blida 2.) (Algeria)
✉ email@email.com
https://orcid.org/0009-0001-7744-8474

Received: 21/10/2025 **Accepted**: 19/5/2026 **Published**: 5/6/2026

Abstract: This study aims to explore the importance of having a digital environment characterized by cyber resilience in protecting academic data of university institutions published on websites, especially in light of increasing threats and security challenges such as hacking and cyber intrusions

To achieve the objectives of the study, the descriptive-analytical approach was adopted to address the issue. The finding syndicate that cyber resilience provides an integrated framework that includes formulating strategies in the field of cybersecurity to assess, detect early, and respond to cyber risks, as well as to recover operations in case of data breaches. It is also essential to develop policies and programs for research, development, and innovation in order to build a high level of security for IT infrastructures and networks that meet safety standards for protecting academic data in Algerian universities

Keywords: Cyber resilience, protection, academic data, Algerian universities.
JEL Classification Codes: L86, K24, C80, I23

* *Corresponding Author.*

Doi: https://doi.org/10.34118/jeemr.v10i1.4597

1. مقدمة :

يتمتع قطاع التعليم العالي والبحث العلمي حاليا بميزة العمل على شبكة الانترنت من خلال رقمنة أنظمة معلومات متنوعة وبرامج متكاملة من جميع المستويات تتيح الوصول للمعلومات والاتصال والتعامل مع الزيادة الهائلة للبيانات، التي باتت عرضة لمجموعة متنوعة من التهديدات كسرقة البيانات أو إتلافها أو إصابة الكومبيوتر بالفيروسات، مما جعل المؤسسات الجامعية مسؤولة عن الفضاء الالكتروني الخاص بها لحماية هذه البيانات المفتوحة من الناحية المادية والأكاديمية، وإحداث توازن بين توافر البيانات من جهة وسلامتها من جهة أخرى، وهذا من خلال تبني نظام المرونة السيبرانية القائمة على اتخاذ تدابير الوقاية والحماية للبيانات ضمن البيئة الرقمية ومراعاة طبيعة التهديدات السيبرانية التي تعترض الخصوصية، وهذا باعتبارها منهج إداري جديد يعالج المخاطر الناجمة عن التهديدات السيبرانية سواء من الناحية المادية أو المعرفية وإعطاء القدرة على التنبؤ والتكيف السريع والمستمر مع هذه التهديدات المحتملة والتعافي من الآثار السلبية للهجمات الالكترونية.

كما سمح تطور مجال تكنولوجيا المعلومات والاتصال للعديد من المتفاعلين بالمشاركة في قواعد البيانات الأكاديمية للمؤسسات الجامعية، مما أدى إلى توليد كم هائل من المعلومات العامة والشخصية عن المستخدمين لشبكة الانترنت بالجامعات بما فيها هويتهم ومعلوماتهم الشخصية التي تحفظ وتخزن وتحلل لاستخدامها حسب الحاجة إليها، هذا ما جعل مستخدمي الشبكة عرضة لمخاطر حتمية تتعارض ومبدأ الحرية الشخصية، لذا بات من الضرورة الحفاظ على أمن البيانات والحفاظ على توفرها ودرجة موثوقيتها، وهذا باتخاذ الإجراءات الأمنية المناسبة التي يمكن أن تساهم في ضمان النتائج المتوقعة وتقليص الاختراقات للبيانات والحد من التلاعب بها وحماية مستخدمي شبكة الانترنت، الأمر الذي جعل مؤسسات التعليم العالي والبحث العلمي الجزائرية تركز على موضوع الأمن السيبراني ليكون من أولوياتها الأساسية وتتخذ أفضل الممارسات والحلول الذكية لتنتقل من مفهوم الأمن السيبراني إلى مفهوم المرونة السيبرانية لضمان حماية البيانات الأكاديمية وتعزيز جاهزيتها لمواجهة التعقيدات والمخاطر السيبرانية ضمن بيئة رقمية غير مستقرة، من خلال هذا يمكننا طرح الإشكالية التالية:

إلى أي مدى تعتبر المرونة السيبرانية آلية فعالة في حماية البيانات الأكاديمية بالجامعات الجزائرية؟

❖ **الأسئلة الفرعية:**

- ماذا نقصد بالمرونة السيبرانية؟ وما هي أبعادها؟
- ما المقصود بحماية البيانات الأكاديمية؟ وما هي مبادئها؟
- ما واقع تبني استراتيجية المرونة السيبرانية بالجامعات الجزائرية؟

❖ **أهداف الدراسة:**

تستهدف هذه الدراسة إبراز مفهوم حماية البيانات الأكاديمية بالجامعات الجزائرية ومبادئ حماية تداولها الكترونيا، وكذا بيان أهمية المرونة السيبرانية ودورها في الحفاظ على البيانات الأكاديمية من المخاطر

التي تهدد أمنها وسلامتها وتحقيق الأمن السيبراني الذي أصبح من المجالات المعقدة التي تحتاج إلى فهم مختلف التهديدات السيبرانية والتدابير الواجب اتخاذها لحماية البيانات.

❖ **أهمية الدراسة:**

تكتسب الدراسة أهمية كبيرة في الوقت الذي بدأت فيه المؤسسات الجامعية تتجه نحو توظيف التكنولوجيا الرقمية في العملية التعليمية باعتبارها موضوع حديث وذلك لما توفره هذه التكنولوجيا من مزايا في تحسين المخرجات الجامعية وزيادة تدفق البيانات على شبكة الانترنت، مما يستوجب ضرورة توفير حماية للبيانات الأكاديمية من المخاطر السيبرانية وتوفير نظام بيئي رقمي مرن.

❖ **منهج الدراسة:**

استخدمت هذه الدراسة المنهج يعطي دفع لمعالجة الموضوع محل الدراسة من جميع جوانبه وتحليل عناصره لتوضيح الأسس النظرية التي تركز عليها المؤسسات الجامعية في إرساء فلسفة المرونة السيبرانية في حماية البيانات الأكاديمية عند التعامل ضمن البيئة الرقمية للجامعات.

❖ **محاور البحث:**

- **المحور الأول:** مفهوم المرونة السيبرانية.
- **المحور الثاني:** الإطار النظري لحماية البيانات الأكاديمية بالمؤسسات الجامعية.
- **المحور الثالث:** دور المرونة السيبرانية في حماية البيانات الأكاديمية بالمؤسسات الجامعية.

2. مفهوم المرونة السيبرانية.

يعود جذور كلمة مرونة إلى علم الفيزياء وعلوم المادة حيث تشير فيه المرونة إلى خاصية المادة، ثم استخدم هذا المصطلح في العلوم الطبيعية والبيطرية لتحديد مجموعة من المعايير القابلة للقياس التي تحدد إمكانية التنبؤ، كما ظهر هذا المصطلح بعد ذلك في علم البيئة الذي يدل على استمرارية الأنظمة وقدرتها على امتصاص الاضطرابات والعودة إلى حالة التوازن، ثم انتقل إلى مجال علم النفس في السبعينات من القرن التاسع عشر والذي اعتبرها كوسيلة للتركيز على عوامل الخطر ونتائجها السلبية على الصحة العقلية ودراسة قوة الشخصية واتخاذ الأشكال الايجابية للتكيف مع عوامل التخفيف والتأثيرات الوقائية، أما المرونة السيبرانية فهي مفهوم جاء كخطوة لاحقة بعد تأسيس قواعد الأمن السيبراني باستخدام الانترنت في السبعينات من بداية القرن الواحد والعشرين، فما المقصود بالأمن السيبراني والمرونة السيبرانية.

1.2. تعريف المرونة والأمن السيبراني:

تعريف المرونة بأنها "وجود القدرة على التغيير أو تغيير بسهولة وفقا للموافق". (الزبيدي، 2021، صفحة 39)

أما المرونة السيبرانية تعرف بأنها: القدرة على الاستشعار والاستعداد الوقائي لمواجهة التهديدات السيبرانية ومقاومتها والرد عليها سواء كانت تلك الأخطار متوقعة أو غير متوقعة، بما يمكن من القدرة على التعافي السريع من آثارها في وقت مناسب.)الصادق(01 .p ,2024 ,

كما تُعرف بأنها: إدارة الخروقات الناجحة والتعامل معها.) هاثاواي(06 .p ,2024 ,

وتُعرف أيضا بأنها: قدرة الأنظمة على توقع المخاطر المحتملة والتكيف معها. (kott & Igor , 2018, p. 3)

وتعرف بأنها: قدرة المؤسسات على الاستمرار في تنفيذ مهمتها من خلال توقع التهديدات السيبرانية والتكيف مع التغيرات الأخرى ذات الصلة في البيئة والصمود واحتواء الحوادث السيبرانية والتعافي منها بسرعة. (باولاك، 2021، صفحة 78)

كما تعرف بأنها القدرة على الاستعداد والتخطيط للأحداث السلبية واحتوائها والتعافي منها والتكيف معها بفعالية أكبر. (kott & Igor , 2018, p. 03)

أما الأمن السيبراني فيعرف بأنه تطبيق والتقنيات والضوابط لحماية الأنظمة الجامعية من الهجمات الالكترونية، (الألفي، 2022، صفحة 818) ويعرف بأنه التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الالكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، بهدف الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحماية خصوصية وسرية البيانات، (السمحات، 2020، صفحة 09)

من خلال التعريفات السابقة يمكن القول أن الامن السيبراني والمرونة السيبرانية يهدفان الى حماية البيانات، غير أن الامن السيبراني يقوم على حماية البيانات من التهديدات بمنع الهجمات السيبرانية قبل وقوعها، أما المرونة السيبرانية فتهدف الى حماية البيانات والتفاعل مع الهجمات السيبرانية عند وقوعها والتكيف والاستجابة لها والتعافي منها بعد وقوعها

2.2.أهمية المرونة السيبرانية: تعمل المرونة السيبرانية على توفير الحماية من كل أشكال التهديدات لسيبرانية خلال تشكيل استراتيجيات دفاعية وخطط قوية لتقليل المخاطر في مواجهة هذه التحديات والمخاطر المحتملة، تبني التخطيط المستمر لدعم استمرارية العمليات، فضلا عن ذلك توفر القدرة على العودة للوضع الطبيعي بعد الاختراق، كما تركز المرونة على الاستباقية في تطوير دفاعها من خلال التوعية بأمن المعلومات والتعليم والتدريب المستمرين، والنسخ الاحتياطي للمعلومات والتعلم من الحوادث السيبرانية السابقة، كما تهدف المرونة السيبرانية للوصول إلى القدرة على تحديد وحماية والكشف عن أي تهديد ينتج عن التعامل عبر شبكة الانترنت والاستجابة والتعافي منه.)روبودين(01 .p ,2024 ,

3.2.مكونات المرونة السيبرانية: تضم المرونة السيبرانية مجموعة من العناصر وتتمثل في:

1.3.2.الحوكمة: إن التطور السريع لبيئة المخاطر السيرانية يؤكد ضرورة تبني نهج قائم على مواكبة هذه المخاطر وتصميم الحوكمة الالكترونية بصورة صحيحة، وتطويرها من الناحية العملية بوضع اتجاهات مستقبلية واسعة لحوكمة المخاطر، وسن القوانين الجديدة لخصوصية البيانات. (عمر، شوفان، و اخرون، 2023، صفحة 17).

2.3.2.التخطيط والاستعداد: وهي مجموعة من الأنشطة التي تتخذ قبل حدوث الهجمات السيبرانية، فهي تعكس مدى جاهزية واستعداد المؤسسات لمواجهة الأخطار السيبرانية والوقاية من آثارها السلبية.

3.3.2.التحليل: تعمل المؤسسات على تحليل الحوادث السيبرانية وتصنيفها حسب نوع الاختراق(فشل العملية أو فشل النظام...)، والجهة الفاعلة له(هواة، ناشطو القرصنة،...) وناقله (برنامج ضار أو فيروس،...) واهم أثاره (انقطاع الخدمة أو توفرها أو تسريب البيانات،...)،وقناة التسليم (بريد الكتروني أو متصفح الويب، أو وسائط التخزين،...) وتقييم مدى خطورة الهجمات السيبرانية بالإضافة إلى تصنفها من الناحية التنظيمية أو القانونية ويتسنى للمؤسسات تحديد الأولويات وتسخير الموارد لتحقيق الاستجابة الفورية والفعالة. (board، 2020، الصفحات 07-10)

4.3.2.الاحتواء: يتمثل في إعداد الوسائل اللازمة لتقليل الضرر الحاصل بعد وقوع الاختراق السيبراني للبيانات وحماية باقي البيانات التي لم تخترق وفق برامج حماية فاعلة.

5.3.2.التعافي: هو عبارة عن مجموعة من الإجراءات التي تهدف إلى استعادة الثقة في الأنشطة عبر شبكة الانترنت بعد حدوث الهجمات السيبرانية والعودة إلى الوضع الطبيعي (الزبيدي، 2021، صفحة 18)

6.3.2.التنسيق والاتصال: تقوم المؤسسات بالتنسيق مع أصحاب المصلحة أو الأطراف المعنية الداخلية والخارجية لتعزيز المرونة والحفاظ على الوعي بالمواقف السيبرانية ضمن البيئة الرقمية، وتتيح لأصحاب المصلحة تقييم الخطورة واتخاذ الإجراءات اللازمة عند حدوث الاختراقات في الوقت المناسب لمعالجتها وتنفيذ خطط الاستجابة والتعافي للمحافظة على دقة وسلامة البيانات. (board، 2020، صفحة 14)

7.3.2. التحسين: يقصد به اكتساب الخبرة الأمنية في مجال الأمن السيبراني من خلال الهجمات السيبرانية السابقة، وهذا قصد تطوير القدرات الأمنية وتحسين المهارات لمواجهة مثل هذه المخاطر مستقبلا. (الزبيدي، 2021، صفحة 18)

4.2. مستويات تطبيق نظام المرونة السيبرانية: لبناء نهج متسلسل للمرونة السيبرانية يكون من خلال ثلاث مستويات كما هي موضحة حسب الشكل الموالي وهي: (kott & Igor , 2018, p. 15)

الشكل 1: المتضمن مستويات المرونة السيبرانية

Source : (kott & Igor , Cyber resilience of systems and networks, 2018, p. 14)

1.4.2.مستوى يتضمن نماذج الفحص لتحديد التحسينات السهلة والتركيز على المزيد من التحليل: يعتمد هذا المستوى على تحليل بسيط وسرعة للمخاطر وبتكلفة أقل يوفر حلول حسب الأولويات للوظائف والمهام عند حدوث الاختراق، ويستخدم تحليل الوصف للبيانات الموجودة والنماذج المفاهيمية.

2.4.2. مستوى تفصيل النماذج عن طريق تحليل القرارات وإعطاء الأولويات للأداء النظامي والاستثمار: يصف هذا النموذج العملية أو نموذج المسار الحرج من خلال تحديد الأحداث المتسلسلة عند حدوث الاختراق وتحديد الانحرافات عن طريق التغذية العكسية.

3.4.2.مستوى النمذجة المعقدة للتفاعلات بين الأنظمة الفرعية واستخدام تحليل التصورات (السينورهات): يكون المستوى الثالث نموذج مفصلا عن الوظائف والمهام والأنظمة الفرعية كل عملية وكل مكونات النظام لجمع المعلومات الكافية لتحديد الاستثمارات في المشاريع القابلة للتنفيذ لتحسين نظام المرونة السيبرانية في المؤسسات وهذا في ظل توافر الموارد المتاحة من قبل صناع القرار.

3. الإطار النظري لحماية البيانات الأكاديمية:

تخزن مؤسسات التعليم العالي والبحث العلمي ملايين السجلات الخاصة بالموظفين والطلاب والأساتذة والخرجين بالإضافة إلى البيانات البحثية العديدة التي تحفظ في قواعد بيانات، والتي يتم الولوج إليها عبر الانترنت، مما يستلزم توفير حماية لها، ولهذا سنتطرق إلى مفهوم البيانات ومبادئ حمايتها.

1.3. تعريف حماية البيانات الأكاديمية:

قبل التطرق إلى مفهوم حماية البيانات نتناول تعريف البيانات والتي تعرف بأنها: كل ما يمكن توليده ومعالجته وتخزينه ونقله بواسطة تقنية المعلومات، كأرقام وحروف ورموز وما إليها، (راضي، 2022، صفحة 51) كما تعرف بأنها مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف الثابتة أو الفيديوهات أو التسجيلات الصوتية أو الرموز التعبيرية. (الاصطناعي، 2024، صفحة 04).

وتُعرف حماية البيانات بأنها: قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم. (الموسي و جان سيربل ، 2013، صفحة 06)

كما يُعرف بأنها: "تنفيذ الوسائل الإدارية أو الفنية أو المادية المناسبة لحماية الكشف غير المصرح به عن البيانات، أو تعديلها أو إتلافها بقصد أو بدون قصد". (يس و أمالي، 2022، صفحة 156)

وتُعرف بأنها: "عملية الكترونية أو تقنية لكتابة البيانات الأكاديمية أو تجميعها أو تسجيلها أو حفظها أو تخزينها باستخدام وسيط من الوسائط أو الأجهزة الالكترونية أو التقنية سواء تم ذلك جزئيا أو كليا" (رجب، 2024، صفحة 426)

2.3. خصائص البيانات الرقمية الأكاديمية: تتمثل خصائص البيانات الرقمية الأكاديمية في النقاط التالية: (الموسي و جان سيربل ، 2013، صفحة 18)

- يتم الحصول عليها بطريق مشروع وقانوني؛
- تستخدم للغرض الأصلي المعلن والمحدد ولا تكشف لغير المصرح لهم الاطلاع عليها؛

- تتصل بالغرض المقصود من جمعها ولا تتجاوزه ومحصورة لذلك؛
- صحيحة تخضع لعمليات التحديث والتصحيح؛
- يتوفر حق الوصول إليها أو الإخطار بأنشطة المعالجة أو النقل وحق التصحيح والتعديل وحتى طلب الإلغاء؛
- تحفظ سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المعالجة؛
- تتلف عند استيفاء الغرض من جمعها.

3.3. مبادئ حماية البيانات الأكاديمية: تعتمد حماية البيانات على مجموعة من المبادئ نذكر منها: (الاصطناعي، 2024، صفحة 07)

- **المسؤولية:** تقع مسؤولية توثيق البيانات وإجراءات الخصوصية على الجامعات؛
- **الشفافية:** يتم معالجة البيانات الأكاديمية بصفة محددة وواضحة وصريحة من خلال وضع إجراءات الخصوصية من طرف الجامعات؛
- **الاختيار والموافقة:** يتم تحديد جميع الخيارات في الحصول على البيانات سواء بصفة ضمنية أو صريحة فيما يتعلق بجمع البيانات واستخدامها؛
- **الحد من جمع البيانات:** يقصد بجمع البيانات الأكاديمية على الحد الأدنى من البيانات التي تحقق لأغراض محددة؛
- **الحد من استخدام البيانات والاحتفاظ بها والتخلص منها:** تقيد معالجة البيانات الأكاديمية للأغراض المحددة لها في إشعار الخصوصية لصاحب البيانات بالموافقة عليها ضمنيا أو صريحة والاحتفاظ بها طالما كان ذلك ضروريا لتحقيق الأغراض المحددة وإتلافها بطريقة آمنة عند عدم الحاجة إليها؛
- **الوصول إلى البيانات الأكاديمية:** يتم تحديد توفر الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إليها؛
- **الحد من الإفصاح عن البيانات الأكاديمية:** تعد الموافقة الضمنية أو الصريحة للإفصاح عن البيانات الأكاديمية للأطراف الخارجية لاستخدامها للأغراض المحددة لذلك؛
- **أمن البيانات:** يتم حماية البيانات الأكاديمية من التسرب أو الفقدان أو الاختلاس أو إساءة استخدامها أو الوصول غير المصرح به وفق التشريعات والقوانين الخاصة بالأمن السيبراني للجامعات.
- **جودة البيانات:** يتم الاحتفاظ بالبيانات الأكاديمية بصورة دقيقة وذات علاقة مباشرة بالأغراض المحددة لذلك؛
- **المرافقة والامتثال:** تضع الجامعات بيانات وإجراءات لمعالجة الاستفسارات والشكاوى النزاعات المتعلقة بالخصوصية.

4.3.أهم المخاطر التي تهدد البيانات الأكاديمية: تتعرض البيانات الأكاديمية على مستوى الجامعات للعديد من المخاطر السيبرانية من أبرزها: (الألفي، 2022، الصفحات 742-743)

التصيد الاحتيالي: غالبا ما تأخذ عملية التصيد شكل رسالة بريد الكتروني أو رسالة فورية تكون مصممة لخداع المستخدم وكسب ثقته بالمصدر محاولة بذلك الوصول إلى بياناته.

برامج الفدية (برامج الضارة): تمنع هذه البرامج المستخدمين من الوصول إلى الشبكة أو الملفات أو البيانات الخاصة بهم مما يتسبب في حدوث مشكلات استرجاع هذه البيانات أو الملفات، وغالبا ما يكون الهدف من هذه البرامج الحصول على فدية مالية لاستعادة البيانات المسروقة من قبل المخترقين.

الاختراق: يؤدي ضعف برامج الحماية أو عدم توفرها إلى سهولة نفاذ المخترقين إلى البيانات الأكاديمية في كافة الأنشطة ضمن البيئة الرقمية والتحكم فيها من خلال معرفة كلمة المرور أو أرقام الأمان للمستخدمين.

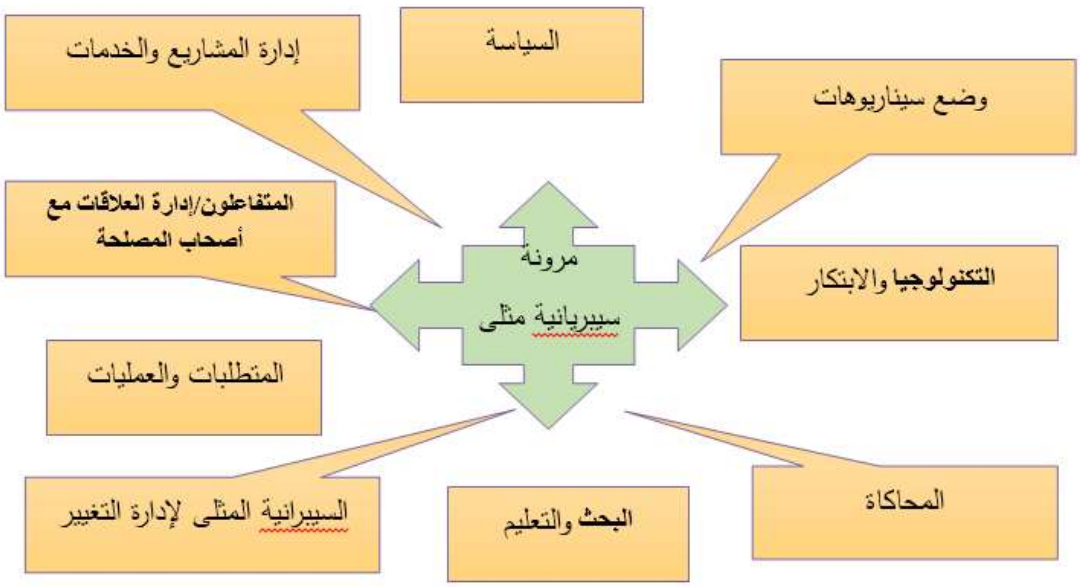
4.دور المرونة السيبرانية في حماية البيانات الأكاديمية بالمؤسسات الجامعية في الجزائر.

أصبحت الهجمات السيبرانية أكثر تعقيد وأكبر استهدافا لقطاع التعليم العالي وهذا لتدفق بياناتها عبر شبكة الانترنت، مما يتعين على المؤسسات الجامعية في الجزائر أن تفكر في كيفية حماية بياناتها الأكاديمية وتخزينها عند التفاعل مع أنظمة الكومبيوتر والشبكات من خلال وضع السياسات والاستراتجيات وإدارة الاختراقات والتنبؤ بها والتعافي منها بكفاءة وفعالية.

1.4. عناصر نظام المرونة السيبرانية المثالي لحماية البيانات الأكاديمية بمؤسسات التعليم العالي بالجزائر:

يتكون النظام المرونة السيبراني المثالي مجموعة من العناصر الموضحة حسب الشكل الموالي:

الشكل رقم (02): نظام المرونة السيبراني الفعال



Source : (shalamanov, 2019, p. 58)

– **السياسات:** تعتبر السياسة الإجراءات الضرورية للحفاظ على مبادئ خصوصية البيانات عن طريق السماح للمؤسسة بالتشغيل السليم لعملياتها من خلال وضع حدود السلوك، حيث يجب على المؤسسة النظر في إنشاء سياسة لحماية البيانات بالحفاظ على حقوق المعني بالبيانات المعمول بها وإدارة الاختراق كما

يجب وضع إجراءات واضحة ومفصلة وإعلانها للأطراف ذات الصلة في جميع أنحاء المؤسسة لضمان الامتثال.

– **البحث والتعليم:** إن تطوير القدرات الأكاديمية للمورد البشري في مجال الأمن السيبراني وتدريبه يوفر الخبرة اللازمة لتعديل قدرة المؤسسات الجامعية على الاستعانة بموظفين أكاديميين ذوي خبرة تساهم في تحسين المرونة السيبرانية خاصة في الحالات الحرجة كما أن لها تأثير ايجابي لمرونة البنى التحتية على مستوى الجامعات.

– **متطلبات وعمليات المرونة السيبرانية:** يتطلب نظام المرونة ضمان توفر البنية التحتية القادرة على تحمل مختلف السيناريوهات والتحديات، وكذا تقييم قدرة تحمل بنيتها بما في ذلك الشبكات والخوادم والأصول المادية الأخرى، (الحسناوي، 2024، صفحة 49)، كما يعتمد هذا النظام على عملية تقييم المخاطر الداخلية والخارجية ثم تحديد الأولويات حسب حجم المخاطر وتطوير إجراءات الاستجابة والتكيف معها في الوقت المناسب بتغيير السياسات وتطبيق الحوكمة بشكل مستمر ودائم باستخدام التقنيات الرقمية كالذكاء الاصطناعي، (shalamanov، 2019، صفحة 62)

– **المحاكاة:** محاكاة التصيد الاحتيالي أو اختبار الاختراق يكون من خلال سلسلة من التدريبات العملية التي تستهدف شبكة المؤسسات الجامعية الجزائرية وأنظمتها ومواردها البشرية لتحديد أوجه الضعف وقياس مستويات الامتثال للسياسات والإجراءات وتقييم فعالية الدفاعات وإجراءات التعافي من الهجمات السيبرانية، فتكون أكثر فعالية عندما تكون مصحوبة بخدمات مثل تحديد نقطة اتصال واضحة لشبكة البيانات واستخدامها للإبلاغ عن الرسائل المشبوهة وهذا لحماية بياناتهم. (كاييخاس، عفيفي، و اخرون، 2021، صفحة 47)

السيناريوهات: يتطلب نظام المرونة السيبرانية صياغة العديد من السيناريوهات للدفاع عن البيانات الأكاديمية للجامعات منها إجراءات محاكاة مختلفة للهجمات السيبرانية وتطبيق آلية الاستجابة للحوادث الطارئة بدء من الاستعداد والاكتشاف والتحليل والاحتواء والتعافي وإجراءات ما بعد الحاجة لإيجاد الحلول المبتكرة لمواجهة هذه التحديات، كما تم وضع سيناريوهات لبرامج الفدية التي تمنع الوصول إلى الملفات والبيانات، وكذا وضع محاكاة للنطاقات السيبرانية التي تعترض نجاح المهاجمين في إرسال بريد تصيد احتيالي. (النعيمي، 2024، صفحة 01)

التكنولوجيا والابتكار: تؤدي التكنولوجيا الحديثة دورا قويا في رسم استراتيجيات واضحة لحماية البيانات والأنظمة الحيوية للجامعات من الهجمات الالكترونية، وتعزيز المرونة السيبرانية من خلال استخدام التقنيات المتقدمة كالذكاء الاصطناعي وتحليل البيانات الضخمة في تحسين القدرة على اكتشاف ومكافحة التهديدات السيبرانية مثل الكشف عن أنشطة غير مشروعة عبر الشبكة. (Admin، 2025، صفحة 01)

–**إدارة المشاريع والخدمات:** إن تقديم الخدمات يتطلب دمج التدابير الأمنية في جميع مراحل تقديم الخدمة بما يشمل حماية البيانات وتأمين الوصول والتوعية بالتهديدات مع استخدام التكنولوجيا أو التقنيات المناسبة وضمات توفير أدوات الحماية الجيدة

-**المتفاعلون وإدارة العلاقات مع أصحاب المصلحة:** تركز إدارة العلاقات على إقامة الشراكات وتبادل المعلومات مع الجهات الخارجية للجامعات لتعزيز القدرة الجماعية على اكتشاف التهديدات السيبرانية ومنعها والاستجابة لها. (الحسناوي، 2024، صفحة 46)

السيبرانية المثلى لإدارة التغيير: تعتبر إدارة التغيير حجر الأساس للمرونة السيبرانية في إدارة المخاطر وتنظيم عملية التغيرات المطلوبة لشبكة انترنت المؤسسات الجامعية، مع ضمان الحفاظ على ضوابط أمن البيانات بتقديم تقييم شامل لهذه المخاطر وتحديد نقاط الضعف وخطة العمل وتحديد الهدف من التغيير، كما تعكس إدارة التغيير الفعالة، بشكل استباقي لتقليل من احتمالية وقع الحوادث الأمنية عند تداول البيانات على شبكة الانترنت (What is Change Management in Cybersecurity? System Integrity,، 2025، صفحة 01).

2.4.أبعاد المرونة السيبرانية في حماية البيانات الأكاديمية المؤسسات الجامعية الجزائرية

تحقق المؤسسات الجامعية الجزائرية المرونة في حماية البيانات الأكاديمية من خلال الأبعاد التالية: (Dupont، 2019، الصفحات 05-08)

- **المرونة الديناميكية:** تتطلب المرونة السيبرانية مجالا زمنيا واسعا يشمل الأنشطة قبل وأثناء وبعد الهجمات السيبرانية، أي انه لا يمكن تحقيق المرونة إلا من خلال عملية دورية تراكمية شبه دائمة تستعد فيه المؤسسات إلى مواجهة مجموعة متنوعة من المخاطر السيبرانية التي تختلف حسب شدتها وتواترها قبل الاختراق، ونشر سياسات وقائية يمكن أن تقلل من تعرضها للمخاطر، وتنفيذ برتوكولات الكشف والاستجابة لتخفيف من الآثار السلبية أثناء عملية اختراق البيانات، وأخيرا تقوم بتكييف نظمها وإجراءاتها لاستيعاب الدروس المستفادة بعد عملية الخرق.

- **المرونة مترابطة:** تعزز المرونة من خلال دمج المؤسسات الجامعية بنظمها الاجتماعية والتقنية بشبكة كثيفة من الروابط داخلها وفيما بينها لتقوية الثقة وتنشيطها وتوفير الموارد وخبرات إضافية في مجال الطوارئ، فيكتسي هذا الترابط الشبكي للمرونة أهمية حيوية لدى المؤسسات الجامعية عند مواجهتها للهجمات السيبرانية والأحداث السلبية التي تمس الهياكل الأساسية والحيوية، ويجب أن تكون هذه الشبكات قادرة على سد الفجوات المادية والمعلوماتية والمعرفية والاجتماعية.

- **المرونة قابلة للممارسة:** إن معالجة أزمة سيبرانية ما لا تبدأ من العدم بل تكون نتيجة لجهود التخطيط الشامل لتطوير مهارات التجسس وزيادة القدرة والثقة الشخصية وتعزيز روابط الشبكة للمؤسسات الجامعية، فالمرونة نهج لظروف غير متوقعة وإدارة هذه الظروف يتطلب التفاعل بين الممارسة والإبداع والبنية والمرونة، حيث تقوم الفرق المسؤولة عن الأمن السيبراني بإنشاء نظام أمني بالجمع بين الاختراعات الفردية والتنسيق الجماعي لتحمل المخاطر عند حدوث أي طارئ وهذا يتطلب تحقيق مستوى من الكفاءة والإلمام بمجموعة متزايدة من التقنيات لتجسيد التوازن المثالي بين الإبداع والبنية أو البيئة التنظيمية وعند كثرة الاختراقات السيبرانية يصبح التدريب والممارسة مكونا رئيسيا للمرونة.

– **المرونة قابلة للتكيف:** تعتبر الأشكال الأكثر تقدما للمرونة التي تشمل الخصائص التكيفية وتقوم على إعادة تخصيص الموارد بسرعة وتطوير ثقافة ملائمة للمواجهة وتفويض عملية صنع القرار فتصبح أكثر استعداد لمواجهة المخاطر غير المتوقعة، وتحقيق المرونة والاستجابة اللازمتين لمعالجة الظروف الجديدة والصعبة من خلال التكرار وتنوع التقنيات.

3.4.خطوات تطبيق استراتيجية المرونة السيبرانية في حماية البيانات الأكاديمية بالمؤسسات الجامعية

– **التخطيط الاستراتيجي:** التخطيط الاستراتيجي في الجامعات هو عملية إدارية تبدأ بإعداد وتحديد التوجهات الإستراتيجية ووضع البدائل والخيارات، ثم صياغة الاستراتيجية وإجراءات الدراسة والتقييم الاستراتيجي لتمكين المؤسسات الجامعية من تحسين قدرتها الأمنية في حماية البيانات، ومواكبة التطورات التكنولوجية الرقمية العالمية ومواجهة المخاطر السيبرانية بكفاءة عالية وثبات واستقرار، (القحطاني، 2022، صفحة 126) كما تتولى المحافظة السامية للرقمنة بالجزائر صياغة الاستراتيجية الوطنية للرقمنة بالتنسيق مع كل القطاعات بما يتوافق ومتطلبات أمن الأنظمة المعلوماتية مع الجهات المختصة، فتقوم المحافظة بتعبئة وتنمية المورد البشري والكفاءات في مجال الرقمنة لضمان اليقظة التكنولوجية وتشجيع التعاون مع المؤسسات الدولية المماثلة. (الرئاسي ا.، 2023، صفحة 10)

– **الاحتواء:** يعتمد الاحتواء على إدارة المخاطر وتقييمها ثم وضع الخطوات الواجب اتخاذها على الفور في تقليل تأثير الخرق واحتوائه للحفاظ على البيانات التي لم تخترق بعد من خلال عدة خطوات كإغلاق النظام حتى لا يتم الوصول إلى باقي البيانات، والعمل على استرداد البيانات التي لم يتم اختراقها للحد من الضرر الناجم عن ذلك مثل استخدام النسخ الاحتياطي لاستعادة البيانات أو تغيير كلمة المرور... الخ، القيام بإعداد تقارير حول عملية الخرق وإبلاغ الجهات المتخصصة عن عملية الخرق، بالإضافة إلى طلب مشورة خبراء في مجال الأمن السيبراني، كما وفرت السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي موقعين الكترونيين للرد عن انشغالات وشكاوي المواطنين والهيئات العامة والخاصة وهذا بغرض تأمين نظام المعلومات وقواعد البيانات وضمان اليقظة التكنولوجيا في مجال حماية البيانات وتأثير الحلول المعتمد لمعالجتها مع إدارة الأنظمة التي تضم المواقع الالكترونية والبرامج المعلوماتية لاسيما قواعد البيانات وامن المعلومات والشبكات بالتنسيق مع المكلفين بالأمن المعلوماتي وإعداد البطاقات لضمان السير الحسن للأرضيات التقنية والتجهيزات المعلوماتية. (الرئاسي ا.، 2023، الصفحات 13-14).

– **الاستجابة السريعة:** بعد تعرض البيانات الأكاديمية لعملية الخرق يتوجب على المؤسسات الجامعية القيام بمراجعة الأسباب التي أدت إلى عملية اختراق البيانات، وإبلاغ الجهة المختصة في حماية البيانات لمراجعة عمليات الحماية وتزويدها بالمعلومات مع تحديد المشكلات المرتبطة بنقاط الضعف في العمليات والإجراءات الأمنية التي تسبب الخرق، وهذا لصياغة خطط عمل مناسبة واتخاذ الإجراءات التي من شانها تصحيح المشكلات وتعمل على تحسين عملية حماية البيانات الأكاديمية. (إفريقيا، 2021، الصفحات 17-18)

– **التعافي المرن:** إن اتخاذ المؤسسات الجامعية لتدابير الوقاية من الهجمات السيبرانية يستوجب بناء خطط واستراتيجيات قوية للتعافي من الآثار السلبية للاختراق والتقليل من انتهاك البيانات.

– **بناء وعي ثقافي:** تعتمد إستراتيجية بناء الوعي الثقافي الأمني على توعية الموظفين والمتفاعلين عبر شبكة الويب للبيئة الجامعية مما يساعد على حمايتها وتكوين خط الدفاع الأول ضد الهجمات السيبرانية، وتتكون هذه الإستراتيجية من الخطوات التالية:

- التدريب: تقوم المؤسسات الجامعية الجزائرية بإجراء دورات تدريبية منتظمة حول التهديدات السيبرانية الشائعة مثل التصيد الاحتيالي والبرامج الضارة وتقديم جلسات حول ممارسات الإدارة المرن والبريد الالكتروني وطرق التصفح الآمن وتقديم أمثلة عن عمليات المحاكاة حتى يتسنى للموظفين والمتفاعلين من فهم وتحديد المخاطر السيبرانية المحتملة والاستجابة لها بشكل أفضل.
- تنفيذ سياسات كلمة المرور القوية: التشجيع على استخدام كلمات المرور المعقدة لتعزيز الأمان والتأكد من أهمية تحديث كلمات المرور بانتظام.
- تعزيز ثقافة الإبلاغ: إن الرفع من مستوى الوعي والثقافة الأمنية يشجع كل الأطراف المتفاعلة مع شبكة البيانات الجامعية على الإبلاغ الفوري عن الأنشطة المشبوهة أو الحوادث المحتملة عن طريق رسائل البريد الالكتروني.
- تحديث البرامج والأنظمة بانتظام: إن تحديث البرامج وأنظمة التشغيل والتطبيقات حسب المستجدات الآمن السيبراني وهذا لسد الثغرات الأمنية.
- تعزيز ممارسات العمل الآمنة عن بعد: يجب التأكيد على استخدام الشبكات الخاصة الافتراضية للاتصالات الآمنة وقنوات الاتصال المشفرة وطرق المشاركة الملفات الآمنة وتوفير إرشادات حول تامين الشبكات والأجهزة لتقليل مخاطر السيبرانية غير المصرح بها.

– **التعاون في مجال الأمن السيبراني:** تعمل المؤسسات الجامعية بالجزائر على تعزيز التعاون وتبادل المعرفة في مجال الأمن السيبراني مع الجهات المختصة، وهذا بإنشاء منصات تبادل المعلومات تعزز ثقافة الانفتاح والاستفادة من الخبرات الدولية لمواجهة الهجمات السيبرانية المعقدة، كما يتيح التعاون جمع الموارد والرؤى وأفضل الممارسات، مما يؤدي إلى خلق استراتيجيات وحلول أكثر فعالية في حماية البيانات الأكاديمية. (كابيتال، 2024، صفحة 03)

5. تحديات جاهزية الجامعات الجزائرية لتبني استراتيجية المرونة السيبرانية:

يواجه تبني المرونة السيبرانية في الجامعات الجزائرية العديد من الصعوبات نذكر منها: (الحسناوي، 2024، صفحة 39)

– تتطور طبيعة التهديدات السيبرانية بتطور التقنيات التكنولوجية وطرق استخدامها مما يجعل توفير الحماية السيبرانية باستمرار أمر صعبا، إضافةً الى كثرة المخترقين وتعددهم أمام البيانات الأكاديمية الجامعية؛

– تعتبر محدودية الموارد المالية والتقنية لاستثمار البنية التحتية السيبرانية وقلة خبرة الكوادر البشرية عائقا امام الجامعات في تنفيذ استراتيجية المرونة السيبرانية لحماية البيانات الاكاديمية،

–إن نقص وصعوبة صياغة التشريعات والقوانين الجامعية لحماية البيانات يعيق جهود تطبيق المرونة السيبرانية في الجامعات الجزائرية؛

– ضعف التنسيق بين المؤسسات الجامعية والمنظمات الوطنية للأمن السيبراني.

6.خاتمة:

تعتبر المرونة السيبرانية أحد المفاهيم الأساسية التي تدور حول نهج التنبؤ ضد الهجمات السيبرانية وانتهاكات البيانات الأكاديمية الموجودة على شبكة الانترنت، لتكون بذلك عبارة عن جسر بين دعم عمليات النظام بإدارة البيانات وتخزينها ونقلها وضمان سرية البيانات والحفاظ على معايير الجودة في الحماية، كما تشير إلى استعداد النظام الرقمي لأي هجوم سيبراني من خلال استراتيجيات وخطوات وإجراءات تحتاج إلى فن استخدماها لتوفير الحماية للشبكات والأجهزة والبيانات، وإرساء بيئة أكثر وعيا بالأمن والقدرة على تحمل الصدمات الخارجية والتعافي منها والتكيف مع الأحداث المستقبلية غير المتوقعة وهذا نتيجة لاعتماد الجامعات على استخدام التكنولوجيا الرقمية.

❖ **النتائج:**

- تشكل الهجمات الالكترونية تهديدا للمؤسسات الجامعية في ظل عملها ضمن النظام الرقمي؛
- تقييم المرونة السيبرانية المخاطر والتهديدات السيبرانية وتحدد مواطن القوة والضعف لسد الاختراقات؛
- تتيح المرونة السيبرانية وضع خطة عمل مناسبة لإدارة الأزمات السيبرانية وحماية البيانات الأكاديمية بصفة مستمرة في جميع المستويات والهياكل؛
- تعمل المرونة السيبرانية على زيادة قدرة المؤسسات الجامعة على مواجه التغيرات البيئة الرقمية السريعة بكفاءة وفعالية مع تمكنها من حماية البيانات في ظل كل الظروف؛
- يتم حماية البيانات الأكاديمية بتفعيل النسخ الاحتياطي التلقائي ووضع برامج حماية والعمل على تحديثها باستمرار؛
- إرساء ثقافة ووعي بالأمن السيبراني للجامعات من خلال التوعية وحماية الوصول إلى البيانات الرقمية؛
- تعكس المرونة السيبرانية الاستجابة لحوادث الخروقات السيبرانية على البيانات الأكاديمية.

❖ **التوصيات:**

- ضرورة تبني أنظمة دفاع الكتروني قوي لحماية البيانات التي تراعي إتباع نهج قائم على أساس تقييم المخاطر السيبرانية والتنبؤ بها؛
- العمل على وضع إستراتيجية واضحة تقوم على فهم البيئة الرقمية وتحليل التهديدات المحتملة لخرق البيانات؛
- وضع منهجية متقدمة لتنفيذ خيارات معالجة المخاطر السيبرانية؛
- وضع تدابير تشريعية وتنظيمية تعزز حماية استخدام البيانات وتداولها عبر الانترنت للمؤسسات الجامعية؛

- تطوير وتنمية قدرات الكوادر البشرية لتستجيب لحالات الطوارئ في مجال الأمن السيبراني من خلال حملات التوعية والتدريب المهني والبحث والتطوير؛
- وضع نموذج أمن البيانات يتيح التنبؤ وسرعة الاستجابة للمخاطر السيبرانية للمؤسسات الجامعية؛
- ضرورة تعزيز التعاون الدولي في مجال سد الهجمات السيبرانية باعتبارها جرائم عابرة للحدود من أجل تأمين حماية البيانات الأكاديمية؛
- إشراك القطاع الخاص والمجتمع المدني في وضع نظام للمرونة السيبرانية يتضمن أمن وحماية البيانات.

6. قائمة المراجع:

–.alexender kott و ،linkov Igor .(2018) . Cyber resilience of systems and networks, fundamental concepts of cyber resilience : introduction and overview .london :springer. 10.1007/978-3-319-77492-3_1

–.Benoıˆt Dupont .(2019) .The cyber-resilience of financial institutions .:Journal of Cybersecurity ،(01)05 ،

–Financial stability board .(2020) .effective practices for cyber incident response and recovery .suisse.

–.Velizar shalamanov .(2019) .organising for it effectiveness efficiency and cyber résilience in the academic sector :national and régional dimensions . Information & Security: An International Journal.62 ،42 ، https://doi.org/10.11610/isij.4203

–.What is Change Management in Cybersecurity? System Integrity ,01 15) ., 2025https://www.vivantio.com/blog/what-is-change-management-in-cyber-security./). تم الاسترداد من

. (01 01, 2025). ،التكنولوجيا والقيادة في الأمن السيبراني: استخدام الابتكار لتحسين الأمن السيبراني. تم Admin–. / ،.https://arab-coaching.comالاسترداد من

–المرسوم الرئاسي رقم 23–314 . (06 09, 2023). المتضمن إنشاء المحافظة السامية للرقمنة وتحديد مهامها وتنظيم سيرها. الجريدة الرسمية الجمهورية الجزائرية، العدد 59، الصادرة في 2023/09/10.

–المرسوم الرئاسي رقم 23–73 . (04 02, 2023). المتضمن تحديد مهام الامانة التنفيذية للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وكيفيات وتنظيمها وسيرها. الجريدة الرسمية الجمهورية الجزائرية، العدد 10، الصادرة في 2023/02/15.

–الهيئة السعودية للبيانات والذكاء الاصطناعي. (04 09, 2024). سياسة حماية البيانات الشخصية. تم الاسترداد من https://sdaia.gov.sa/ar/SDAIA/about/Files/RegulationsAndPolicies02.pdf.

– Īmān ʻAbd al-Ḥamīd Yāsīn, wa Muḥammad al-Sayyid Amālī. (2022). Ḥimāyat al-bayānāt al-shakhṣīyah bi-al-maktabāt al-Jāmiʻīyah fī Miṣr dirāsah istikshāfīyah. al-Majallah ʻilmīyah Maḥkamat (32)

-باتريك باولاك. (2021). توقعات كبيرة، أجندة الأمن السيبراني عبر البحر الأبيض المتوسط. المعهد الاروبي للبحر الأبيض المتوسط.

-جمهة النعيمي. (05 10, 2024). سبع تمارين وسيناريوهات للأمن السيبراني، . تم الاسترداد من https://www.aletihad.ae/news. /

-خورخي فلوريس كاييخاس، عائشة عفيفي، و اخرون. (2021). الأمن السيبراني في مؤسسات منظومة الأمم المتحدة، الأمم المتحدة: الامم المتحدة.

-روبودين. (06 08, 2024). المرونة السيبرانية- بديل أم مكمل له. تم الاسترداد من https://robodin.com/cyber-resilience./

- سامر محمد عمر، سلام شوفان، و اخرون. (2023). تحقيق المرونة في الأمن الالكتروني من نهج قائم على تحليل المخاطر. انجلتر: أرنست ويونغ.

- عادل عبد الصادق. (05 08, 2024). المرونة السيبرانية والتنمية المستدامة في العصر الرقمي. تم الاسترداد من https://accaronline.com/article detail.aspx?id=37896.

- عمار عبد الحسين شعلان الحسناوي. (2024). استراتجية المرونة السيبرانية ودورها في تعزيز ثقة المودعيين. مذكرة ماجيستير. كلية الإدارة والاقتصاد، جامعة كربلاء: العراق.

- عمر ابو عرقوب. (04 09, 2024). واقع الخصوصية وحماية البيانات الرقمية في فلسطين دراسة استكشافية . تم الاسترداد من https://7amleh.org/storage. %/

- فاستر كابيتال. (09 10, 2024). صياغة خطة قوية للاستجابة للحوادث للشركات الناشئة. تم الاسترداد من https://fastercapital.com/arabpreneur.

- فاطمة بنت محمد بن سابق القحطاني. (2022). استراتجيات الأمن السيبراني وتطبيقها بالتخطيط الاستراتجي لمواجهة الإرهاب الالكتروني في جامعة الأميرة نورة بنت عبد الرحمن: تصور مقترح، المؤتمر الدولي لمكافحة الإرهاب الالكتروني، 04، المملكة العربية السعودية: جامعة المملكة العربية السعودية.

- Umm. M. shmym Muzhir Rāḍī. (2022). al-Ḥaqq fī Ḥimāyat al-bayānāt al-shakhṣīyah fī ẓill al-Dustūr Jumhūrīyat al-‘Irāq li-sanat 2005. Majallat Jāmi‘at al-Imām Ja‘far al-Ṣādiq, 37 (07)

- مجموعة الامتثال لمحاكمة الجرائم المالية في منطقة الشرق الأوسط وشمال إفريقيا. (2021). دليل علمي لإنشاء إطار عمل للخصوصية وحماية البيانات. تم الاسترداد من https://menafccg.com/wp-content/uploads ، / تاريخ الاطلاع 2024/09/30،

- محمد جعفر الزبيدي. (2021). المرونة الاستراتجية وتأثيرها في إدارة الأزمات الأزمات دراسة استطلاعية تحليلية لآراء القادة العاملين في محافظة مكافحة إجرام بغداد. مذكرة ماجيستير. كليةالادارة والاقتصاد، جامعة كربلاء: العراق.

- مليسيا هاثاواي. (05 08, 2024). إدارة الخطر السيبراني الوطني. تم الاسترداد من hyyps://potomacinstitute.org/images/CRI/Managing-Nationl-Cyber-Risks FINAL-Arabic.pdf.

- Muná Turkī al-Mūsá, wa Faḍl Allāh, Jān syrbl. (2013). Khuṣūṣīyat al-ma‘lūmāt wa-ahammīyatuhā wa-makhāṭir al-Tiqnīyāt al-ḥadīthah ‘alayhā,,. Majallat Kullīyat Baghdād lil-‘Ulūm al-iqtiṣādīyah al-Jāmi‘ah, 2013 (24), 06.

- Muná ʻAbd Allāh alsmḥāt. (2020). Mutaṭallabāt taḥqīq al-amn alsybrāny al-anẓimah al-maʻlūmāt al-Idārīyah bi-Jāmiʻat al-Malik Saʻūd. Majallat al-Tarbiyah (111), 09

-.Hānī Rizq ʻAbd al-Jawwād al-Alfī. (2022)., al-qiyādāt al-Akādīmīyah wa-adwāruhā fī taʻzīz mumārasāt al-amn alsybrāny bi-al-jāmiʻāt al-Amrīkīyah wa-imkānīyat al-Ifādah minhā bi-al-jāmiʻāt al-Miṣrīyah,. Majallat Kullīyat al-Tarbiyah, Jāmiʻat al-Manṣūrah (114), 10. 21608 / maed. 2022. 269212

.- Hibat Ramaḍān Rajab. (2024). al-Ḥimāyah al-qānūnīyah llbyānāt al-shakhṣīyah fī ʻaṣr al-tiknūlūjiyā al-raqmīyah,. 66, Miṣr : al-Kullīyah al-Ḥuqūq bi-Jāmiʻat ʻAyn al-shams al-munʻaqid fī al-rābiʻ wa-al-khāmis min Nūfimbir 2023.