جامعة غرداية

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

بالتعاون مع مخبر أبحاث البنية الرقمية والذكاء الاصطناعي وتطبيقاتهما في التحول الرقمي للقطاعات الاقتصادية.

وبالإشتراك مع فرقة بحث متطلبات تطبيق حوكمة الشركات والتدقيق المحاسبي في المؤسسات الإقتصادية الجزائرية بمخبر الدراسات التطبيقية في العلوم المالية.

وبالإشتراك مع النقابة الوطنية المستقلة لمستخدمي التعليم العالي - فرع غرداية، ينظمون:

الملتقى الوطني الأول (حضوري وعن بعد) حول: حوكمة مؤسسات التعليم العالي

في ظل التحول الرقمي والتشريعات الحديثة.

مداخلة بعنوان:

الأمن السيبراني وحماية البيانات كمتطلب أساسي لحوكمة الجامعات في العصر الرقمي

من إعداد الباحثين :

من خلال المحور رقم: 04

- **عبد الرؤوف عباده، أستاذ، جامعة غرداية،** abada.abderraouf@univ-ghardaia.edu.dz
- **بن طجين محمد عبد الرحمان، أستاذ محاضر أ، جامعة غرداية،** bentadjine.abderrhmane@univ-ghardaia.edu.dz
- **باي محمد أيوب، طالب دكتوراه، جامعة غرداية،** bey.mohamed.ayoub@univ-ghardaia.edu.dz

الملخص:

تهدف هذه الدراسة إلى إبراز الدور الجوهري للأمن السيبراني في تفعيل مبادئ حوكمة الجامعات ضمن سياق التحول الرقمي الذي يشهده قطاع التعليم العالي في الجزائر. تنطلق الدراسة من إشكالية مفادها أن الرقمنة الشاملة للأنظمة البيداغوجية والإدارية (مثل نظام PROGRES) لا يمكن أن تحقق أهدافها في الشفافية والمساءلة ما لم تكن محصنة بمنظومة أمنية تضمن خصوصية وسلامة البيانات. وباعتماد المنهج الوصفي التحليلي، واستعراض مجموعة من الدراسات السابقة المتخصصة، خلصت الدراسة إلى أن الأمن السيبراني يمثل الركيزة التقنية للحوكمة الرشيدة، وأن حماية الأصول الرقمية والمعرفية للجامعة هي ضمانة لسيادتها العلمية. وتوصي الدراسة بضرورة صياغة استراتيجية وطنية للأمن السيبراني الجامعي، تعتمد على الذكاء الاصطناعي وتوطين البيانات في سحب وطنية سيادية، مع تعزيز الوعي الرقمي لدى كافة منتسبي

Abstract:

This study aims to highlight the vital role of cybersecurity in activating the principles of university governance within the context of the digital transformation in the Algerian higher education sector. The study addresses the problem that the comprehensive digitalization of pedagogical and administrative systems (such as the PROGRES system) cannot achieve its goals of transparency and accountability unless it is fortified by a security system that ensures data privacy and integrity. By adopting a descriptive-analytical approach and reviewing a set of specialized previous studies, the study concludes that cybersecurity represents the technical pillar of good governance, and that protecting the university's digital and intellectual assets is a guarantee of its scientific sovereignty. The study recommends the necessity of formulating a national strategy for university cybersecurity, relying on artificial intelligence and localizing data in national sovereign clouds, while enhancing digital awareness among all university members.

Keywords: Cybersecurity; University Governance; Data Protection; Digital Transformation; Higher Education.

1. مقدمة:

يشهد العالم المعاصر تحولا جذريا في بنية المؤسسات التعليمية، حيث فرضت الثورة الصناعية الرابعة على الجامعات الانتقال من نمط الإدارة التقليدي إلى "الحوكمة الرقمية". هذا الانتقال لم يعد مجرد رفاهية تقنية، بل أصبح ضرورة حتمية لضمان كفاءة الأداء الأكاديمي والإداري. ومع اعتماد الجامعات على الأنظمة السحابية، وقواعد البيانات الضخمة (Big Data)، ومنصات التعليم عن بُعد، برزت تحديات أمنية معقدة تهدد استقرار هذه المؤسسات.

إن مفهوم حوكمة الجامعات يقوم في جوهره على مبادئ الشفافية، المساءلة، وسيادة القانون. وفي ظل الرقمنة الشاملة، تصبح هذه المبادئ في مهب الريح ما لم تكن مسيجة بنظام متين للأمن السيبراني. فالبيانات الجامعية — التي تشمل السجلات الأكاديمية للطلاب، وبحوث أعضاء هيئة التدريس، والبيانات المالية، وبراءات الاختراع — تمثل "الأصول الرقمية" الأكثر قيمة، والتي باتت هدفاً مستمراً للهجمات السيبرانية وبرمجيات الفدية.

تأتي هذه الدراسة لتسلط الضوء على العلاقة العضوية بين الأمن السيبراني كمنظومة تقنية، والحوكمة كإطار إداري وقانوني. فالحوكمة الرشيدة في العصر الرقمي تتطلب صياغة استراتيجيات استباقية لإدارة المخاطر الرقمية، وضمان خصوصية البيانات كجزء لا يتجزأ من جودة التعليم العالي. ومن هنا، تبرز الحاجة الملحة لتحديد المتطلبات الأساسية التي يجب أن تتبناها الجامعات لتأمين فضائها الرقمي، بما يتماشى مع التوجهات الوطنية الرامية إلى الرقمنة الشاملة وحماية السيادة المعلوماتية.

إشكالية البحث:

تتمحور إشكالية هذه الدراسة حول التساؤل الجوهري التالي: **"إلى أي مدى يشكل الأمن السيبراني وحماية البيانات الركيزة الأساسية لتفعيل**

نموذج حوكمة الجامعات في ظل التحول الرقمي الراهن؟" وينبثق عن هذا التساؤل أسئلة فرعية:

1. ما هو الإطار المفاهيمي لحوكمة الجامعات في ظل البيئة الرقمية؟
2. ما هي أبرز المخاطر السيبرانية التي تهدد استمرارية المرفق الجامعي وحرمة بياناته؟
3. كيف يمكن بناء استراتيجية حوكمة رقمية توازن بين تدفق المعلومات وحمايتها؟

أهمية الدراسة:

تستمد الدراسة أهميتها من كونها تعالج موضوعاً يتقاطع فيه التقني بالإداري، حيث تسعى لتقديم رؤية تأصيلية لدور الأمن السيبراني في حماية "السمعة الأكاديمية" للمؤسسة، وامتثالها للتشريعات القانونية الحديثة (مثل القانون 18-07 في الجزائر المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي).

الداسات السابقة

تجمع الدراسات السابقة على أن الأمن السيبراني لم يعد مجرد خيار تقني، بل هو الركن الأساسي لنجاح استراتيجية رقمنة قطاع التعليم العالي. فبناءً على ما ورد في دراسة (عباسي و حفيظي، 2022)، فإن الرقمنة هي "المُمكن" الحقيقي لحوكمة الجامعات، حيث تساهم في أرشفة المسارات البيداغوجية وعصرنة التسيير الإداري عبر منصات رقمية متكاملة. ومع ذلك، فإن هذا التحول الرقمي الشامل يضع الجامعة أمام "انكشاف سيبراني" خطير؛ وهنا تتقاطع دراسة (حميدي و طاليب ، 2022) مع واقع الجامعة الرقمية، لتؤكد أن تأمين هذه المنصات هو ما يمنح الحوكمة طابعها "الموثوق"، فبدون أمن سيبراني تتحول الرقمنة من أداة للتطوير إلى ثغرة لاستنزاف البيانات.

وفي ظل توجه وزارة التعليم العالي نحو تعميم الأنظمة المدمجة (مثل نظام PROGRES والمنصات التعليمية Moodle)، تبرز أهمية دراسة (زمورة و بن عيسى،

2022) التي تشدد على "حوكمة الأمن" كشرط للتحول الرقمي الآمن. ففي البيئة الجامعية، لا تقتصر الحماية على البيانات المالية فقط -كما في دراسة (دلامي و يونسي ، 2025) الخاصة بالبنوك- بل تمتد لتشمل "السيادة العلمية" وحماية الملكية الفكرية، وهو ما يجعل توصيات (قوي، 2019) بشأن الصيانة الأمنية الدورية ضرورة قصوى لمنع تعطل المرافق الرقمية الجامعية.

علاوة على ذلك، فإن رقمنة قطاع التعليم العالي في الجزائر تواجه تحديات "الجوسسة والاختراقات" التي فصلتها دراسة (كلاع، 2022)، خاصة وأن الجامعات أصبحت مستودعات ضخمة للبيانات الشخصية والبحثية. وهذا ما يستوجب تفعيل المقاربة التي طرحتها دراسة (جودي، 2025) حول استخدام الذكاء الاصطناعي لتأمين السحب الجامعية الوطنية. إن الفجوة التي يسدها البحث الحالي تكمن في كونه ينقل مفاهيم الحوكمة من إطارها الإداري العام كما في دراسة (عباس، 2019) ليضعها في قلب "المختبر الرقمي للجامعة"، مؤكداً أن نجاح التحول الرقمي الأكاديمي مرهون بقدرة المؤسسة على الموازنة بين الانفتاح الرقمي والانضباط السيبراني.

2. الإطار المفاهيمي لحوكمة الجامعات والأمن السيبراني

يقتضي البحث العلمي أولاً تحديد المصطلحات بدقة، خاصة وأن "الحوكمة" و"الأمن السيبراني" مفهومان متداخلان في البيئة الرقمية الجامعية.

أولا: مفهوم حوكمة الجامعات (University Governance)

جوكمة الجامعات عبارة عن قدرة الجامعات على التحكم والسيطرة على جميع العمليات الإدارية بطريقة علمية رشيدة، وخطط فاعلة وأساليب مناسبة لتحقيق أهدافها، بمستوى عال الجودة، وتحسين أدائها (شنافي ، 2021، صفحة 19).

كما تعرف حوكمة الجامعات بأنها مجموعة من النظم والقواعد التي تضبط العلاقة بين الأطراف الفاعلة في المؤسسة الأكاديمية (الإدارة، الأستاذ، الطالب، والبيئة الخارجية). وفي العصر الرقمي، انتقل المفهوم من "الحوكمة الورقية" إلى "الحوكمة الرقمية" (E-Governance)، والتي تتميز بـ:

- الشفافية الرقمية: إتاحة الوصول إلى المعلومات والنتائج والقرارات عبر المنصات الإلكترونية.
- المساءلة الإلكترونية: القدرة على تتبع العمليات (Logs) وتحديد المسؤوليات في حال حدوث خلل.
- الاستجابة: سرعة تقديم الخدمات الجامعية رقمياً (مثل التسجيلات والطعون).

ثانيا: ماهية الأمن السيبراني (Cyber Security)

الأمن السيبراني هو ذلك النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات 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 لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إل خسائر دائمة (بارة ، 2017، صفحة 257)

والأمن السيبراني في الوسط الجامعي ليس مجرد "تثبيت مضاد فيروسات"، بل هو منظومة متكاملة لحماية الشبكات، الأجهزة، والبرامج من الهجمات الرقمية. ويتضمن ثلاثة أبعاد رئيسية:

1. البعد التقني: الوسائل الدفاعية كالتشفير (Encryption) والجدران النارية.
2. البعد التنظيمي: السياسات والبروتوكولات التي تحدد من يملك صلاحية الدخول للبيانات.
3. البعد البشري: وعي المستخدم (أستاذ أو طالب) بكيفية التعامل مع التهديدات.

ثالثا: حماية المعطيات كجوهر للحوكمة

المعطيات ذات الطابع الشخصي هي كل معلومة بغض النظر عن داعامتها متعلقة بشخص معرف او قابل للتعرف عليه (الشخص المعني : كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة.) بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية او الجينية او البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية (السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، 2025، صفحة 3)

كما تعتبر البيانات هي "النفط الجديد" للجامعات. وتشمل المعطيات التي تعالجها الحوكمة الجامعية:

- البيانات الشخصية: الأسماء، العناوين، الأرقام الوطنية، والحسابات البنكية للموظفين.
- البيانات الأكاديمية: كشوف النقاط، شهادات التخرج، ومحتوى المحاضرات.
- البيانات البحثية: نتائج المخابر العلمية والأبحاث التي لم تنشر بعد.

3. واقع التهديدات السيبرانية وتداعياتها على الحوكمة الجامعية

إن انفتاح الجامعة على الفضاء الرقمي جعلها "مؤسسة زجاجية" أمام الهجمات السيبرانية المتطورة. لم تعد التهديدات مجرد فيروسات بسيطة، بل تحولت إلى "حروب معلوماتية" تستهدف البنية التحتية الأكاديمية.

أولا: تصنيف التهديدات السيبرانية في الوسط الجامعي

يمكن تقسيم التهديدات التي تواجه الجامعات إلى ثلاثة أصناف رئيسية:

1. **الهجمات التقنية (Technical Attacks):**
   - **هجمات حجب الخدمة (DDoS):** استهداف منصات التعليم الإلكتروني (مثل Moodle) لإخراجها عن الخدمة، خاصة في فترات الامتحانات أو التسجيلات، مما يضرب مبدأ "التوافر" في الحوكمة.
   - **برمجيات الفدية (Ransomware):** تشفير قواعد بيانات الجامعة (النقاط، البحوث) والمطالبة بمبالغ مالية، وهو ما يهدد استمرارية المرفق العام.
2. **هجمات الهندسة الاجتماعية (Social Engineering):**
   - استغلال قلة الوعي لدى الموظفين أو الطلاب للحصول على كلمات المرور عبر "التصيد الاحتيالي" (Phishing)، وهي الثغرة الأكثر خطورة في الجامعات.
3. **التهديدات الداخلية (Insider Threats):**
   - سواء كانت ناتجة عن إهمال (فقدان وحدة تخزين) أو تعمد (تلاعب موظف أو طالب بالنتائج)، وهذا يمس مباشرة بمبدأ "المساءلة".

ثانيا: تداعيات الاختراقات على حوكمة الجامعة

إن نجاح أي هجمة سيبرانية يؤدي إلى انهيار منظومة الحوكمة من عدة جوانب:

- **فقدان المصداقية والسمعة (Reputational Damage):** عندما يتم تسريب بيانات الطلاب أو تزوير الشهادات، تفقد الجامعة مكانتها في التصنيفات الدولية وثقة الشركاء الاجتماعيين.
- **الخسائر المادية والمعرفية:** ضياع سنوات من البحوث العلمية الممولة أو اضطرار الجامعة لدفع تكاليف باهظة لاسترجاع الأنظمة.
- **المسؤولية القانونية:** في ظل قوانين حماية البيانات الحديثة، تصبح الجامعة مسؤولة قانوناً عن أي تقصير في حماية خصوصية منتسبيها.

ثالثا: تحديات الأمن السيبراني في الجامعات الجزائرية

بالإشارة إلى السياق الجزائري، تبرز تحديات خاصة:

- الاعتماد المتزايد على الرقمنة المركزية (مثل نظام PROGRES).
- نقص الكوادر المتخصصة في "الأمن الدفاعي" داخل المصالح التقنية للجامعات.
- الحاجة إلى تحيين الترسانة القانونية الداخلية للجامعات لتواكب الجرائم الإلكترونية المستحدثة.

4. المتطلبات الأساسية لحماية البيانات كركيزة لحوكمة الجامعات

إن الانتقال إلى "الجامعة الذكية" يفرض استبدال آليات الرقابة التقليدية بآليات رقمية قادرة على الصمود أمام التهديدات. وبناءً على ما طرحته دراسة (زمورة و بن عيسى، 2022، صفحة 424) حول حوكمة الأمن السيبراني، يمكننا حصر المتطلبات الأساسية في ثلاثة مستويات متكاملة:

أولا: المتطلبات التنظيمية والإدارية (المستوى الهيكلي)

حوكمة الجامعات تعني في جوهرها "توزيع الصلاحيات والمسؤوليات". وفي العصر الرقمي، يتطلب ذلك:

1. **صياغة "ميثاق الأمن السيبراني الجامعي":** وهو وثيقة إدارية تحدد سياسات الوصول إلى البيانات. هذا المطلب يجسد مبدأ الشفافية والمساءلة الذي طرحته (عباس، 2019، صفحة 146)، حيث يجب أن يعرف كل مستخدم (أستاذ، طالب، إداري) حقوقه وحدوده الرقمية.
2. **استحداث وحدة "إدارة المخاطر الرقمية":** لا يمكن تحقيق الحوكمة دون هيئة رقابية. يجب أن تضم الجامعات خلايا تقنية متخصصة تابعة لرئاسة الجامعة مباشرة، تقوم بمهام "التدقيق الرقمي" المستمر، تماشياً مع رؤية (قوي، 2019، صفحة 102) حول ضرورة العمل على ضمان أمن المعلومات وشبكات الأنترنت.
3. **تصنيف البيانات الجامعية:** المتطلب التنظيمي يفرض تصنيف المعلومات إلى (بيانات عامة، بيانات داخلية، بيانات سرية ككشوف النقاط وبراءات الاختراع)، وتطبيق بروتوكولات حماية متفاوتة الشدة لكل صنف.

ثانيا: المتطلبات التقنية والبرمجية (المستوى الدفاعي)

بناء على دراسة (حميدي و طاليب ، 2022، صفحة 10) حول تهديدات الأمن السيبراني، تتحدد المتطلبات التقنية للجامعة في:

1. تأمين الهوية الرقمية (IAM): من خلال استخدام "المصادقة ثنائية العوامل" (2FA) للولوج إلى نظام PROGRES أو منصات Moodle. هذا الإجراء يمنع انتحال الشخصية ويضمن أن "المساءلة" تقع على الشخص الصحيح.
2. تشفير البيانات (Data Encryption): يجب أن يتم تشفير كافة قواعد البيانات الحساسة (سجلات الامتحانات، البيانات المالية) لمنع قراءتها في حال حدوث اختراق مادي للخوادم، وهو ما يضمن "نزاهة البيانات" (Data Integrity).
3. الاستثمار في الذكاء الاصطناعي الدفاعي: كما أشارت دراسة (جودي، 2025، صفحة 103) يجب على الجامعات تبني أنظمة (IDS/IPS) تعتمد على الذكاء الاصطناعي للكشف عن الأنماط غير الطبيعية في تدفق البيانات، مما يسمح بصد الهجمات قبل وقوعها.

ثالثا: المتطلبات القانونية والامتثال (المستوى التشريعي)

الحوكمة هي "سيادة القانون"، وفي الفضاء الرقمي الجامعي الجزائري يتجسد ذلك في:

1. الامتثال للقانون 18-07: المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. يجب أن تلتزم الجامعة رقميا بحماية خصوصية الطالب والأستاذ، وأي تسريب لهذه البيانات يضع الجامعة تحت طائلة المساءلة القانونية والقضائية
2. التوفيق بين الحوكمة والحرية الأكاديمية: وفقا لدراسة (مناصرة، 2023)، تسعى الدول إلى تحقيق حوكمة إنترانت مشتركة وتحقيق حد أدنى من الأمن السيبراني العالمي، وبالتالي يجب أن تكون القوانين الداخلية للجامعة مرنة بما يكفي للسماح بالبحث العلمي، وصارمة بما يكفي لمنع اختراق الخصوصية، وهو ما يسمى بـ "التوازن السيبراني".

5. استراتيجية مقترحة لتعزيز الأمن السيبراني في إطار حوكمة الجامعات الرقمية

إن بناء جامعة ذكية ومحوكمة يتطلب تجاوز الحلول التقنية الظرفية نحو استراتيجية شاملة ومستدامة. بناء على استقراء بعض الدراسات، لاسيما دراسة (جودي، 2025) و (زمورة و بن عيسى، 2022)، نقترح الرؤية التالية:

1. تفعيل نموذج "الحوكمة الاستباقية" عبر الذكاء الاصطناعي

بدلا من انتظار وقوع الاختراق ثم التعامل معه، يجب على الجامعات تبني أنظمة أمنية تعتمد على التعلم الآلي (Machine Learning) للتنبؤ بالهجمات.

- الهدف: حماية "السيادة العلمية" للجامعة من خلال الكشف المبكر عن محاولات التجسس على المخابر والبحوث.
- الآلية: ربط أنظمة الجامعة بمركز عمليات أمنية (SOC) وطني خاص بقطاع التعليم العالي، يقوم بتحليل البيانات الضخمة (Big Data) ورصد التحركات المريبة في الشبكة.

2. مأسسة "الثقافة السيبرانية" كجزء من المواطنة الجامعية

لا يمكن نجاح الحوكمة ما لم يكن "العنصر البشري" واعيا بمسؤوليته. وتتضمن الاستراتيجية هنا:

- **التكوين المستمر:** إخضاع الإطارات الإدارية لتدريبات دورية حول "الأمن الإداري الرقمي"، تماشيا مع ما طرحه حول أهمية الصيانة البشرية قبل التقنية.
- **بناء الوعي الطلابي:** إدراج مقياس "الأخلاقيات الرقمية والأمن السيبراني" ضمن التكوين القاعدي لكل التخصصات، لضمان عدم استغلال ثغرات الطلبة في اختراق شبكات الجامعة.

3. التحول نحو "السحابة الجامعية الوطنية" السيادية

تعتمد الحوكمة الرشيدة على التحكم الكامل في البيانات. لذا، تقترح الدراسة:

- توطين البيانات: التوقف عن تخزين البيانات الجامعية الحساسة في خوادم أجنبية (Cloud الأجنبي) والتوجه نحو سحابة وطنية موحدة تحت إشراف وزارة التعليم العالي.
- حوكمة الولوج: تطبيق سياسة "الوصول الأدنى"بحيث لا يملك أي مستخدم صلاحية الدخول إلا للبيانات الضرورية لمهامه، مما يقلل من مخاطر "التهديدات الداخلية" التي تمت الإشارة إليها في دراسة (كلاع، 2022، صفحة 308).

4. التكامل التشريعي والأخلاقي (ميثاق الرقمنة)

تطوير أطر قانونية داخلية في الجامعات تتواءم مع **القانون 18-07** الجزائري، بحيث يتضمن نظام الجامعة الداخلي عقوبات إدارية وقانونية واضحة ضد أي محاولة للتلاعب بالبيانات الرقمية، مما يعزز مبدأ "المساءلة" الذي هو جوهر الحوكمة (عباس، 2019، صفحة 146)

6. الخاتمة

في ختام هذه الدراسة، يمكن القول إن العلاقة بين الأمن السيبراني وحوكمة الجامعات لم تعد علاقة ثانوية أو مكملة، بل أصبحت علاقة وجودية في ظل البيئة الرقمية المتسارعة. فإذا كانت الحوكمة هي العقل المدبر الذي يضع استراتيجيات الشفافية والمساءلة والنزاهة الأكاديمية، فإن الأمن السيبراني هو الدرع التقني الذي يضمن عدم المساس بهذه المبادئ أو انحرافها عن مسارها الصحيح، كما أن الانتقال نحو "الجامعة الذكية" في الجزائر يتطلب إرادة إدارية تؤمن بأن الاستثمار في الأمن الرقمي ليس تكلفة مالية، بل هو استثمار في استدامة المرفق الجامعي وصون سمعته الأكاديمية في فضاء رقمي لا يعترف إلا بالمؤسسات المحصنة تكنولوجياً ومعرفيا، حيث نستخلص من هذه الدراسة النتائج التالية:

1. الأمن السيبراني هو "العمود الفقري" للحوكمة: لا يمكن الحديث عن شفافية أو جودة في التعليم العالي إذا كانت البيانات عرضة للتزوير أو الضياع.
2. الرقمنة وسيلة والحوكمة غاية: رقمنة الجامعات الجزائرية (نظام PROGRES نموذجاً) حققت نقلة نوعية، لكن استكمال نجاحها مرهون بمدى صمود أنظمتها الأمنية.
3. تكامل الأدوار: حماية البيانات هي مسؤولية تشاركية تبدأ من الأستاذ والطالب وتنتهي بأعلى سلطة إدارية في الجامعة.

التوصيات:

1. إنشاء "قطب وطني للأمن السيبراني الجامعي" يتولى التنسيق بين مختلف الجامعات لتبادل الخبرات والتحذيرات الأمنية.
2. الاعتماد على البرمجيات الحرة والوطنية لتقليل التبعية التكنولوجية وحماية السيادة الرقمية.
3. إجراء تدقيق أمني (Audit) خارجي بصفة دورية ومنتظمة من قبل هيئات وطنية مختصة لتقييم ثغرات الأنظمة الجامعية.
4. الإسراع في إنشاء سحابة وطنية (National Cloud) خاصة بقطاع التعليم العالي لتوطين البيانات وتأمينها سيادياً.
5. تخصيص ميزانية مستقلة ضمن ميزانية الجامعة السنوية خاصة حصرياً بـ "تحديث البنية التحتية للأمن الرقمي".
6. تبني معايير الآيزو (ISO/IEC 27001) كإطار مرجعي لحوكمة أمن المعلومات داخل الجامعات.
7. الرقابة الصارمة على الوصول إلى البيانات الحساسة من خلال تكنولوجيا "البلوكشين" (Blockchain) لضمان عدم قابلية السجلات الأكاديمية للتعديل غير المشروع.

7. قائمة المراجع:

1- يصخشلا عباطلا تاذ تايطعملا ةيامحل ةينطولا ةطلسلا .(2025) *18 نوناقلا*
مقر نوناقلاب ممتملاو لدعملا ،2018 ةنس وينوي 10 يف خرؤملا 07-
صاخشألا ةيامحب قلعتي ، 2025 ويلوي 24 يف خرؤملا 11 - 25

الطبيعين في مجال معلجة المعطيات ذات الطابع الشخصي. تم الاسترداد من https://anpdp.dz/ar/storage/2025/08/18-07-Edited.pdf

2- بوحنية قوي. (2019). الأمن السيبراني والصيانة في المنظمات والحكومات دراسة في المؤشرات والتطبيقات. *مصداقية، 1*(1)، 44-77. تم الاسترداد من https://asjp.cerist.dz/en/article/125953

3- جودي, خ. (2025). هندسة الأمن السيبراني في عصر الذكاء الاصطناعي- قراءة في أدوار واستراتيجيات اليقظة الخوارزمية. *المجلة الجزائرية للأمن الإنساني, 11*(1), 77-110.

4- حميدي , ح., & طاليب , ن. (2022). مدخل مفاهيمي حول الأمن السيبراني. *مدار, 2*(2), 1-16. Récupéré sur https://asjp.cerist.dz/en/article/232540

5- دلامي, م., & يونسي , م. (2025). حوكمة البنوك العمومية الجزائرية كألية لإدارة مخاطر الامن السيبراني في ظل استخدامات الذكاء الاصطناعي – دراسة حالة عينة من البنوك العمومية الجزائرية-. *دفاتر البحوث العلمية, 13*(2), 249-270. Récupéré sur https://asjp.cerist.dz/en/article/278932

6- زمورة , ج., & بن عيسى, ل. (2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر. *مجلة البحوث الاقتصادية المتقدمة, 7*(2), 414-429. Récupéré sur https://asjp.cerist.dz/en/article/203547

7- سمير بارة . (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. *المجلة الجزائرية للأمن الإنساني، 2*(2)، 255-280. تم الاسترداد من https://asjp.cerist.dz/en/article/66092

8- عباس, ز. (2019). حوكمة الجامعات كمدخل لإصلاح التعليم العالي بين حتمية التغيير ومعوقات التطبيق نماذج جامعات دولية في مجال حوكمة. *مجلة دفاتر اقتصادية, 10*(1), 139-162. Récupéré sur https://asjp.cerist.dz/en/article/91917

9- كلاع, ش. (2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني. *مجلة الحقوق والعلوم الانسانية,*

Récupéré sur .314-292 ,(1)*15*
https://asjp.cerist.dz/en/article/186191

10- نوال شنافي . (2021). حوكمة الجامعات: بين المفهوم والتطبيق. *مجلة التغير الاجتماعي، 6*(1)، 13-30. تم الاسترداد من https://asjp.cerist.dz/en/article/216848

11- يزيد عباسي ، و سليمة حفيظي. (2022). الرقمنة كمطلب استراتيجي لتحقيق حوكمة الجامعات الجزائرية. *المجلة الجزائرية للأبحاث والدراسات، 5*(2)، 164-184. تم الاسترداد من https://asjp.cerist.dz/en/article/186894

12- يوسف مناصرة. (2023). التوفيق بين حوكمة الإنترنت والأمن السيبراني للدول. *مجلة صوت القانون، 9*(3)، 315-340. تم الاسترداد من https://asjp.cerist.dz/en/article/221459