

تحليل السياسات والإجراءات الأمنية المتبعة لحماية الخدمات الرقمية في الجامعات الجزائرية: دراسة حالة جامعة المدية

Security policies and procedures adopted to protect digital services in Algerian universities: A field study at the University of Medea.

جامعة ابن خلدون تيارت / الجزائر مخبر البحث: التكنولوجيات الجديدة للمعلومات ودورها في التنمية الوطنية قسنطينة 02، الجزائر	مكتبات وتكنولوجيات الإعلام	كباش الطاهر – طالب دكتوراه (tahar.kabache@univ-tiaret.dz)
جامعة ابن خلدون تيارت / الجزائر مخبر البحث: التكنولوجيات الجديدة للمعلومات ودورها في التنمية الوطنية قسنطينة 02، الجزائر	مكتبات وتكنولوجيات الإعلام	دريخ نبيل – أستاذ التعليم العالي (nabil.derbikh@univ-tiaret.dz)
DOI :		

الإرسال: 2025/04/07 القبول: 2025/05/12 النشر: 2025/06/19

ملخص:

تهدف هذه الدراسة إلى تحليل السياسات والإجراءات الأمنية المتبعة لحماية الخدمات الرقمية في الجامعات الجزائرية، مع التركيز على جامعة المدية كدراسة حالة. يأتي هذا الاهتمام نظرًا للاعتماد المتزايد على الخدمات الرقمية في التعليم العالي الجزائري، وما يرتبط بذلك من حاجة ماسة لتعزيز الأمن السيبراني لمواجهة التهديدات المتعددة، مثل القرصنة، والتصيد الاحتيالي، واختراق البيانات، والبرامج الضارة، وهجمات برامج الفدية.

اعتمدت الدراسة على المنهج التحليلي، حيث تم جمع البيانات من خلال مقابلات مع موظفي تكنولوجيا المعلومات بجامعة المدية، والملاحظة بالمشاركة، واستطلاعات الرأي لموظفي الجامعة والطلاب، بالإضافة إلى مراجعة الأدبيات والوثائق ذات الصلة. وهدفت هذه الأدوات إلى تحديد التهديدات السيبرانية الرئيسية التي تواجه الجامعات الجزائرية وتقييم فعالية الإجراءات الأمنية الحالية.

أظهرت النتائج أن جامعة المدية تطبق سياسات وإجراءات أمنية واضحة لحماية خدماتها الرقمية، وذلك من خلال مركز متخصص في أنظمة المعلومات يعمل على تطوير البنية التحتية الرقمية وتأمينها. كما تقوم الجامعة بتنفيذ إجراءات أمنية فنية وإدارية لضمان سلامة وسرية البيانات، إلى جانب تنظيم برامج توعوية لموظفيها حول أهمية الأمن السيبراني. ومع ذلك، تواجه الجامعة تحديات كبيرة، أبرزها محدودية الموارد المالية، وتعقيد البنية التحتية لتقنية المعلومات، وصعوبة مواكبة التطور السريع في أدوات الهجمات الإلكترونية.

كلمات مفتاحية: الأمن الرقمي؛ السياسات والإجراءات الأمنية؛ الخدمات الرقمية؛ الجامعات الجزائرية؛ جامعة المدينة.

Abstract:

This study aims to analyze the security policies and procedures implemented to protect digital services in Algerian universities, with a focus on the University of Médéa as a case study. This interest stems from the increasing reliance on digital services in Algerian higher education and the associated urgent need to enhance cybersecurity to address multiple threats, such as hacking, phishing, data breaches, malware, and ransomware attacks. The study adopted a descriptive approach, collecting data through interviews with IT staff at the University of Médéa, participant observation, surveys of university staff and students, and a review of relevant literature and documents. These tools aimed to identify the main cybersecurity threats facing Algerian universities and evaluate the effectiveness of current security measures.

The results revealed that the University of Médéa applies clear security policies and procedures to protect its digital services through a specialized information systems center responsible for developing and securing digital infrastructure. The university also implements technical and administrative security measures to ensure data integrity, confidentiality, and availability, alongside organizing awareness programs for its staff on the importance of cybersecurity. However, the university faces significant challenges, including limited financial resources, the complexity of IT infrastructure, and the difficulty of keeping pace with the rapid evolution of cyberattack tools.

Keywords: Digital security; security policies and procedures; digital services; Algerian universities; University of Médéa.

مقدمة:

أصبحت الخدمات الرقمية عنصراً محورياً في حياتنا المعاصرة، حيث تُستخدم على نطاق واسع في مجالات متعددة كالتعليم، والتجارة، والخدمات الحكومية، وغيرها. وفي إطار التعليم العالي، تُعد الجامعات من أبرز المؤسسات التي تعتمد بشكل كبير على الخدمات الرقمية لتلبية احتياجات الطلاب والأساتذة، حيث تشمل هذه الخدمات المنصات التعليمية الإلكترونية، وأنظمة البريد الإلكتروني، والمكتبات الرقمية، والمواقع الإلكترونية للجامعات، وغيرها من الأدوات التي تساهم في تسهيل العمليات التعليمية والإدارية.

مع هذا الاعتماد المتزايد على الخدمات الرقمية، تبرز الحاجة الملحة إلى تأمينها وحمايتها من التهديدات الإلكترونية المتطورة، مثل الاختراقات السيبرانية، وسرقة البيانات الحساسة، والتلاعب بالنظم الرقمية. هذه التهديدات قد تؤدي إلى عواقب وخيمة، بما في ذلك تعطيل العملية التعليمية، وفقدان الثقة في الخدمات الرقمية، وتسريب المعلومات السرية.

لذلك، تُعد السياسات والإجراءات الأمنية التي تعتمد عليها الجامعات لضمان أمن خدماتها الرقمية من الأولويات الاستراتيجية التي تتطلب مراجعة وتطويراً مستمرين. وفي هذا الصدد، يتوجب على الجامعات الجزائرية، على وجه الخصوص، تبني استراتيجيات متقدمة للأمن السيبراني، وتنفيذ سياسات وإجراءات أمنية فعالة لضمان حماية وسلامة خدماتها الرقمية.

للتعرف على السياسات والإجراءات الأمنية المعمول بها لحماية الخدمات الرقمية المتاحة للطلاب والأساتذة قمنا بطرح التساؤل الرئيسي التالي: "ما هي السياسات والإجراءات الأمنية التي تم اتخاذها لحماية الخدمات الرقمية في جامعة المديّة، وما هي التحديات والصعوبات التي تواجهها الجامعة في هذا المجال؟".

منهج الدراسة:

تم تطبيق المنهج التحليلي في هذه الدراسة، حيث استخدمت جامعة المديّة كنموذج للدراسة الميدانية. واستخدمت الدراسة مجموعة متنوعة من أدوات البحث، بما في ذلك المقابلات مع موظفي تكنولوجيا المعلومات بجامعة المديّة والملاحظة المشاركة.

أهداف الدراسة:

- زيادة على محاولة الإجابة على التساؤل الرئيسي لهذه الدراسة، تهدف الدراسة إلى:
- تقييم السياسات والإجراءات الأمنية الحالية في جامعة المديّة وتحديد مدى فعاليتها في حماية الخدمات الرقمية.
- تحديد التحديات والمشاكل التي تواجه الجامعات الجزائرية في تطوير وتطبيق السياسات والإجراءات الأمنية لحماية الخدمات الرقمية.

- تقديم توصيات وإرشادات لتطوير وتحسين السياسات والإجراءات الأمنية في جامعة المدينة والجامعات الجزائرية الأخرى.
 - توفير بيانات ومعلومات عن الأمن الرقمي في الجامعات الجزائرية لتعزيز الوعي الأمني وتعزيز التعاون الإلكتروني بين الجامعات والمؤسسات ذات الصلة.
 - تسليط الضوء على أهمية الأمن الرقمي في الجامعات والمؤسسات التعليمية وتوعية الطلاب والموظفين حول أهمية الالتزام بالسياسات والإجراءات الأمنية لحماية البيانات والمعلومات الحساسة
- الإطار النظري:

1. مفهوم الخدمات الرقمية:

مجموعة من الإجراءات الرقمية المرتبطة ببعضها البعض لأداء وظيفة كاملة تقدم من الجهة الحكومية للمستفيد من خلال القنوات الرقمية مثل البوابات الإلكترونية وتطبيقات الأجهزة الذكية، وتكون ذات مخرج رئيسي واحد معرف ومحدد، ويمكن أن ترتبط مجموعة من الخدمات ببعضها البعض لتكوين منتج رقمي (هيئة الحكومة الرقمية، 2023)، كما يشير مفهوم الخدمات الرقمية إلى توفير مجموعة من الخدمات والمنتجات عبر الإنترنت والأنظمة الرقمية. تشمل هذه الخدمات مثل التسوق عبر الإنترنت، الدفع الإلكتروني، التعليم عن بُعد، والخدمات الحكومية الإلكترونية. توفر الخدمات الرقمية سهولة الوصول والاستخدام للمستخدمين، مما يعزز الكفاءة والتنمية المستدامة (Matar, 2020)

كما تعرف على أنها جميع الخدمات (مثل البيانات والصوت والفيديو) المقدمة من خلال الوسائل الإلكترونية. ويشمل ذلك التقاط المعلومات وتخزينها واسترجاعها ونقلها و / أو الاتصال بها و / أو نشرها إلكترونياً والتقنيات المستخدمة لدعم هذه الأنشطة. تشمل هذه التقنيات الأنظمة والبرامج والأجهزة والاتصالات ومرافق الشبكة. قد يتم استضافة طريقة التسليم داخل مرافق تكنولوجيا المعلومات بالجامعة، خارجياً أو معاً. قد يتم دفعها أو دفعها مجاناً أو الاشتراك فيها أو شراؤها أو تقديمها من خلال السحابة أو كخدمة مُدارة. (Western Sydney University, 2023)

2. السياسات والإجراءات:

مجموعة القواعد والتنظيمات الإدارية التي توضع من خلال الإدارة (كاعوه، 2020)

3. الأمن السيبراني:

الأمن السيبراني هو عملية حماية الأنظمة والبيانات والاتصالات والشبكات الموجودة والمتصلة بالإنترنت ضد الهجمات الرقمية. فهذه الهجمات، التي يشار إليها عادة باسم "الهجمات السيبرانية"، ما هي إلا محاولة اختراق، أو تعديل أو تعطيل أو دخول أو استخدام غير مشروع. وبالتالي، يمكن أن تتراوح الهجمات السيبرانية من تثبيت رموز برمجية ضارة على جهاز حاسوب شخصي وصولاً إلى محاولة تدمير البنية التحتية لدول بأكملها. (المركز الوطني للأمن السيبراني، 2022).

يعني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء خصوصاً بعد الثورة الهائلة في عالم الاتصالات والتداولات الإلكترونية. (الشمري، 2021)

كما أعطى له المشرع الجزائري تعريفاً في الفقرة الثالثة من المادة العاشرة من القانون رقم : 04-18 : بأنه مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة

4. أمن المعلومات

يشير أمن المعلومات إلى مجموعة من الإجراءات والأدوات الأمنية التي تحمي على نطاق واسع معلومات المؤسسة الحساسة من سوء الاستخدام أو الوصول غير المصرح به أو التعطيل أو الإتلاف. يشمل أمان المعلومات الأمن المادي والبيئي والتحكم في الوصول والأمان عبر الإنترنت. غالباً ما يتضمن أمن المعلومات تقنيات مثل وسطاء أمان الوصول إلى

السحابة (CASB)، وأدوات كشف الخداع، والكشف التلقائي والاستجابة على النقط النهائية (EDR)، واختبار الأمان لـ DevOps (DevSecOps) والمزيد. (مايكروسوفت، 2023).

كما يقصد بأمن المعلومات من زاوية أكاديمية العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة.

5. الفرق بين أمن المعلومات والأمن السيبراني:

الرابط بين أمان المعلومات والأمن السيبراني هو علاقة متداخلة جزئياً. تتعامل أمان المعلومات مع حماية المعلومات ضد الوصول غير المصرح به، سواء كانت مستندات ورقية أو محفوظة على وسائط إلكترونية. بيد أنه لا يمكن اعتبار أمان المعلومات متضمناً لأمن الشبكات بشكل كامل، وكذلك لا يتضمن أمن الشبكات أمان المعلومات بالكامل. (قطاف وبوقرين، 2022). الأمن السيبراني يشمل حماية المعلومات المنقولة أو المخزنة أو المعالجة في أنظمة تكنولوجيا المعلومات والاتصالات. ومع ذلك، يتضمن الأمن السيبراني أيضاً الحفاظ على توافر وأمان الخدمات المقدمة عبر الفضاء السيبراني، مثل الكهرباء ووسائل الاتصال. وعليه، لا يمكن القول بأن أمان المعلومات يغطي الأمن السيبراني بأكمله، وكذلك لا يمكن القول بأن الأمن السيبراني يشمل أمان المعلومات بالكامل، حيث لا يتناول أمان المعلومات المكتوبة على الورق، إذ لا يندرج ضمن مجال الفضاء السيبراني. (احمد عبد الكريم وخلف، 2020) لذا، تتقاطع علاقة أمان المعلومات والأمن السيبراني فيما يتعلق بحماية المعلومات الرقمية، لكن تفاوتاتهما تظهر في باقي المجالات المعنية. يجب الانتباه إلى أن أمان المعلومات والأمن السيبراني ليسا مصطلحين مترادفين تماماً

6. الخدمات الرقمية في مؤسسات التعليم العالي:

تشهد مؤسسات التعليم العالي في الجزائر تطورًا ملحوظًا في استخدام التقنيات الرقمية والخدمات الرقمية في العملية التعليمية والإدارية. وفقًا لوزارة التعليم العالي والبحث العلمي (وزارة التعليم العالي والبحث العلمي، بروغرس، 2023)، تعمل الجامعات الجزائرية على تبني وتطبيق هذه الخدمات في مختلف المجالات الجامعية لتسهيل وتحسين العمليات التعليمية والإدارية. ويتم توفير العديد من الخدمات الرقمية في الجامعات الجزائرية لتحسين تجربة الطلاب والموظفين وتيسير إجراءاتهم، ومن بين هذه الخدمات:

6.1. نظام إدارة الجامعة الإلكتروني: وهو نظام يستخدم لإدارة العمليات الأكاديمية والإدارية في الجامعة، والتسجيل في الدورات واختيار المقررات، والإعلان عن النتائج الأكاديمية. (Bin Herzallah, 2021)

6.2. المكتبة الرقمية: وهو نظام يتيح الوصول إلى الكتب والأبحاث والمقالات العلمية عبر الإنترنت. يساعد هذا النظام الطلاب والباحثين على الحصول على المعلومات اللازمة لأبحاثهم ودراساتهم (حسين و توزان، 2021)

6.3. نظام التعليم الإلكتروني: وهو نظام يستخدم لتقديم المحتوى التعليمي عبر الإنترنت، ويتضمن محاضرات مسجلة ومواد تعليمية وتمارين واختبارات عبر الإنترنت. يساعد هذا النظام الطلاب على تعلم المواد بشكل أكثر فاعلية وتفاعلية (Bin Herzallah, 2021)

6.4. نظام البريد الإلكتروني الجامعي: وهو نظام يستخدم للتواصل بين الطلاب والموظفين في الجامعة، ويتضمن إرسال واستقبال الرسائل الإلكترونية والإعلانات الرسمية والإخطارات الأكاديمية. (السيبي، 2023)

6.5. نظام المنصة الإلكترونية لإدارة المشاريع البحثية: وهو نظام يستخدم لإدارة مشاريع البحث وتتبع تقدمها وتحديثها على الإنترنت. يساعد هذا النظام الباحثين على تنظيم عملهم وتحسين تأثير أبحاثهم. (Bin Herzallah, 2021)

بالإضافة لذلك فقد أطلقت وزارة التعليم العالي عدت منصات رقمية لفائدة الطلبة والأساتذة والجمهور من بينها:

منصة بوابة الطالب، منصة تسيير الشهادات الأجنبية، منصة تسجيل للدكتوراه، منصة الخدمات الجامعية، منصة إدارة الموارد البشرية، منصة إدارة البحث، منصة الإدارة المالية والمحاسبية، منصة المستودع المشترك، منصة الشكاوى، (وزارة التعليم العالي والبحث العلمي، بروغرس، 2023) منصة الدفتر التوجيهي المرجعي "التكوين-وظيفة"، منصة متابعة المشاريع المبتكرة، ومنصة "سينما الجامعة" منصة تقييم الباحثين الدائمين منصة الترشح لمنصب مدير الخدمات الجامعية، ومنصة متابعة الممتلكات الخاصة بقطاع التعليم العالي والبحث العلمي، منصة الطالب الأجنبي منصة شبكة التواصل لخريجي الجامعة الجزائرية ALUMNI، منصة تسيير الموارد البشرية و أخرى بإواء الطلبة كما خصصت منصة "أسالي" لفائدة تلاميذ الثانويات و أخرى موجهة لطلبة الدكتوراه من أجل متابعة التكوين الأولي وكذلك منصة لمتابعة استثمارات القطاع و منصة رقمنة المكتبات الجامعية. (وزارة التعليم العالي والبحث العلمي، النشاطات الوزارية، 2023)

7. أهمية أمن البيانات وحماية الخدمات الرقمية في مؤسسات التعليم العالي

أصبح العمل عن بُعد شائعاً بسبب جائحة COVID-19. تواجه العديد من مؤسسات التعليم العالي تحديات أمنية لأنه أصبح إجراء الدروس والعمليات تتم الآن عبر الإنترنت. ومع وجود قوة عاملة مشتتة وهيئة طلابية تعمل عبر الإنترنت، تصبح مؤسسات التعليم العالي عرضة للهجمات الإلكترونية. (HurixDigital، 2023)

كما تقوم الجامعات بتحويل المزيد من أنشطتها عبر الإنترنت، وتتحول إلى حلول مستندة إلى السحابة مع تنفيذ عملية التحول الرقمي. ومع نقل المزيد من البيانات إلى السحابة، يتعرض المزيد من البيانات لخطر الاختراق، ولا يوجد نقص في المهاجمين الذين يتم استغلال الثغرات. وفي ندوة Times Higher Education بالشراكة مع Amazon Web Services، قال ستيف كينيت، المدير التنفيذي للبنية التحتية الإلكترونية والمالك الأول لمخاطر المعلومات العليا في Jisc، إن التحول الرقمي إيجابي بطبيعته ولا يمكن تجنبه، ولكن تنفيذه يطرح سؤالاً حول مخاطر الأعمال. وأضاف: "الأشعار ذكيون مثلنا ويعرفون ماذا يسعون إليه،" مع الترحيل الهائل في العام الماضي إلى العمل عن بُعد، والاستفادة بشكل أفضل من السحابة -وهو أمر جيد -فقد عرض المزيد من البيانات لمزيد من المخاطر،

ولست متأكدًا من أن الجميع على دراية بهذه المخاطر المتزايدة وأن البعض الخطوات البسيطة التي يمكنهم اتخاذها لحمايتها " (Amazon Web Services, 2021).

لذا تحتاج الجامعات، إلى التفكير في إيجاد أكثر الطرق فعالية لتعزيز أمنها. في واقع الأمر، يصبح الأمن أول شيء يجب الاهتمام به ومن أسباب أهمية حماية البيانات والخدمات الرقمية في الجامعات نجد : (Chachak, 2023)

- حماية البيانات الحساسة.

- الحفاظ على الامتثال للتنظيم.

- تجنب فقدان البيانات.

- حماية الملكية الفكرية.

- منع هجمات الإنترنت.

- تقليل الأضرار السمعية.

- إظهار التزام السلامة.

8. التهديدات الأمنية التي تواجه الخدمات الرقمية في الجامعات الجزائرية:

تواجه الجامعات العديد من المخاطر والتهديدات الأمنية عند استخدام الخدمات الرقمية. يمكن أن تؤثر هذه المخاطر على مصداقية الجامعة وسلامة المعلومات الحساسة. فقد كشفت دراسة استطلاعية قام بها كل من Maddy Ell و Robbie Gallucci حول انتهاكات الأمن السيبراني لعام 2022 بالمملكة المتحدة والصادر عن بقسم العلوم والابتكار والتكنولوجيا وقسم الثقافة والإعلام والرياضة بالمملكة المتحدة أن الجامعات هي الأكثر تعرض للهجمات والخروقات السيبرانية بنسبة 92% مقارنة مع مؤسسات الأعمال والمدارس الابتدائية والمدارس الثانوية وكليات التعليم الإضافي (Ell & Gallucci, 2022) علاوة على ذلك، يشير التقرير إلى أن أداء قطاع التعليم العالي ضعيف في تصحيح الإيقاع وأمن الشبكات وأمن التطبيقات، وفيما يلي بعض المخاطر والتهديدات الشائعة:

- 8.1. **هجمات الفدية: (Ransomware)** يمكن للقراصنة استخدام برامج الفدية لتشفير البيانات ومنع الوصول إليها حتى يتم دفع فدية لاستعادة الوصول. تشكل هذه الهجمات تهديدًا كبيرًا للجامعات التي تعتمد على البيانات الرقمية. (Abdulrahman & Omar, 2018)
- 8.2. **هجمات انتحال الهوية: (Phishing)** يمكن للمهاجمين استخدام هجمات البريد الإلكتروني المزيفة لاستهداف الموظفين والطلاب والاستيلاء على بيانات الاعتماد الحساسة. (Naidu & Zainuddin, 2021)
- 8.3. **الخرق الأمني للبيانات:** يمكن أن تؤدي الثغرات الأمنية في الشبكات والتطبيقات إلى تسريب بيانات حساسة مثل المعلومات الشخصية والأكاديمية للطلاب والموظفين. (Fouad, 2021)
- 8.4. **هجمات النفاذ غير المصرح به: (Unauthorized Access)** يمكن للمهاجمين استغلال ثغرات الأمان للوصول إلى الشبكات والأنظمة الرقمية دون إذن (Dicky , 2003).
- 8.5. **الهجمات الداخلية: (Insider Threats)** قد يتسبب الموظفون السابقون أو الحاليون الذين يمتلكون صلاحيات الوصول في تسريب المعلومات الحساسة أو التسبب في أضرار عمدية. (Neetesh , et al., 2020)
- 8.6. **الهجمات الموجهة: (Targeted Attacks)** قد تواجه الجامعات هجمات موجهة من قبل جهات معادية تهدف إلى الحصول على معلومات حساسة أو تعطيل الخدمات الرقمية (Bill & Valerie , 2014).
- 8.7. **الهجمات الناجمة عن الفيروسات والبرمجيات الخبيثة (Viruses and Malware):** يمكن أن تتعرض الأنظمة الرقمية للجامعات للتهديدات الفيروسية والبرمجيات الخبيثة التي تؤدي إلى تلف البيانات أو تعطيل الخدمات. (ليتم و ليطم، 2017)
- 8.8. **الهجمات السيبرانية المتقدمة:** يمكن أن تتعرض الجامعات الجزائرية للهجمات السيبرانية المتقدمة التي تستخدم تقنيات متطورة لاختراق الأنظمة والشبكات الرقمية، مما يمكن أن يؤدي إلى الوصول غير المصرح به إلى البيانات والمعلومات الحساسة (العمرى، 2022)

8.9. التهديدات الخارجية: قد تواجه الجامعات الجزائرية التهديدات الخارجية، مثل الهجمات السيبرانية من مجموعات متطورة أو حكومات أجنبية، والتي يمكن أن تستهدف البيانات والأنظمة الحساسة في الجامعات بهدف الاستفادة منها بطرق غير (مصطفى، 2003، صفحة 15)

8.10. الهجمات المستهدفة على البنية التحتية للشبكات: يمكن أن تتعرض البنية التحتية للشبكات في الجامعات الجزائرية لهجمات مستهدفة تستهدف الخوادم، والشبكات، والأجهزة الأمنية، مما يتسبب في تعطيل الخدمات الرقمية. (Matteo , Alessandro , & Riccardo , 2021)

8.11. التهديدات الناجمة عن الأجهزة المتصلة (IoT Threats): مع زيادة استخدام الأجهزة المتصلة في الجامعات (IoT) ، يمكن أن تتعرض الجامعات للتهديدات الأمان المرتبطة بهذه الأجهزة، مثل اختراق الشبكات والوصول غير المصرح به (Dicky , 2003) .

8.12. التهديدات الناجمة عن الإهمال (Negligence): قد يتسبب الإهمال من قبل المستخدمين في تعريض المعلومات الحساسة للخطر، مثل استخدام كلمات مرور ضعيفة أو عدم تحديث البرمجيات الأمنية (Dicky , 2003) .

8.13. التهديدات الناجمة عن تطبيقات الجيل الثالث (Third-Party Threats): قد تتعاون الجامعات مع جهات خارجية لتوفير خدمات رقمية معينة. إذا كانت هذه الجهات لديها ضعف في أمانها، فقد يؤدي ذلك إلى تعريض الجامعات للمخاطر (Catherine , 2023)

8.14. ضعف التأمين على البيانات: يمكن أن يكون هناك ضعف في التأمين على البيانات أو ضعف سياسات إدارة الهوية والوصول في الجامعات الجزائرية، مما يعرض البيانات الحساسة للتسريب والاستخدام غير المصرح به، ويمكن أن يكون ذلك نتيجة لسياسات ضعيفة لإدارة الوصول وحماية قواعد البيانات،

8.15. ضعف التحديثات الأمنية: يمكن أن يكون هناك تأخر في تطبيق التحديثات الأمنية لأنظمة الجامعات الجزائرية وبرامج الحماية،

8.16. ضعف التوعية الأمنية: يمكن أن يكون ضعف التوعية الأمنية لدى الطلاب والموظفين في الجامعات الجزائرية تهديداً أمنياً، حيث يمكن أن يؤدي إلى

سقوطهم ضحية هجمات احتيالية أو تهديدات سيبرانية بسبب عدم التعرف على
الخطورة واتباع سلوكيات أمان رقي.

8.17. انقطاع الخدمات الرقمية: قد تتعرض الخدمات الرقمية في الجامعات

الجزائرية لانقطاع أو تعطل بسبب أعطال التكنولوجيا، وهذا يمكن أن يؤثر على
توفر الخدمات الرقمية ويعرض البيانات وال

8.18. الاحتفاظ بالبيانات الشخصية: يمكن أن تكون الجامعات الجزائرية

تخزين كم كبير من البيانات الشخصية للطلاب والموظفين، مثل المعلومات
الأكاديمية والمالية والطبية، وهذا يزيد من خطر تعرض هذه البيانات للاختراق أو
الوصول غير المصرح به.

8.19. انتشار التطبيقات والأجهزة الضعيفة: قد يتم استخدام التطبيقات

والأجهزة الرقمية الضعيفة أو الغير محدثة في الجامعات الجزائرية، مما يزيد من
فرص استغلال الثغرات الأمنية واختراق الأنظمة الرقمية.

8.20. عدم وجود آليات احترافية للكشف عن الهجمات: يمكن أن تزيد

عدم وجود آليات احترافية للكشف المبكر عن الهجمات السيبرانية في الجامعات
الجزائرية من تأثيرها السلبي على أمن الخدمات الرقمية.

9. السياسات والإجراءات الأمنية الخاصة بحماية الخدمات الرقمية الجامعية:

تعتبر الخدمات الرقمية الجامعية أحد الأهداف الرئيسية للقراصنة والمخترقين، حيث
يسعون لاختراقها وسرقة المعلومات الحساسة التي تحتوي عليها. ولحماية هذه الخدمات،
يتم اعتماد سياسات وإجراءات أمنية متعددة تهدف إلى تحسين الحماية وتقليل خطر
الاختراق.

يرتكز تطبيق هذه السياسات والإجراءات حول (Matteo , Alessandro , & Riccardo ,
2021) (ليتم و ليتم، 2017) (زهودر، 2021) (Chen, Luo, Shi, Cao, & Zhang, 2023)
:(University of Toronto, 2020) (Office of Information Security, 2023)

- سياسة أمن المعلومات والخدمات الرقمية
- سياسة إجراءات المتعلقة بالأدوار والمسؤوليات

- سياسة الاستخدام المقبول لموارد تكنولوجيا المعلومات والاتصالات
- إرشادات معالجة المعلومات
- إجراءات الاستجابة لحوادث أمن المعلومات
- سياسات وإجراءات تقييم المخاطر
- سياسات وإجراءات التحكم في الوصول
- سياسات وإجراءات التدريب على الوعي الأمني
- سياسات وإجراءات الأمن المادي
- سياسات وإجراءات القانونية لحماية المعلومات والخدمات الرقمية
- سياسات وإجراءات إدارة الأجهزة والشبكات
- سياسات وإجراءات التطوير والتحسين المستمر لأمن المعلومات والخدمات الرقمية

بالإضافة إلى أن أهم السياسات والإجراءات الأمنية المطبقة لضمان أمن المعلومات والخدمات الرقمية في الجامعات، نجد جامعة ويسترن سيدني التي وضعت مجموعة من السياسات والإجراءات الخاصة لحفظ أمن المعلومات والخدمات الرقمية لديها، (Western Sydney University, 2023) تشمل الاستخدام القانوني والأمن للبيانات وتدريب المستخدمين على الممارسات الأمنية. تتضمن الإجراءات حماية البيانات عبر كلمات مرور قوية، وتقييد الوصول وفق مبدأ "أدنى امتيازات"، وضمان استمرارية الخدمات عبر خطط طوارئ. تشرف لجنة الأمن الرقمي (DSSC) على تطبيق هذه السياسات، ومراجعة نظام إدارة الأمن (ISMS) دوريًا، مع توفير وصول آمن عن بُعد وتوعية مستمرة لضمان الامتثال للمعايير الأمنية والقانونية.

10. متطلبات تحقيق الأمن للخدمات الرقمية الجامعية:

تحقيق الأمان للخدمات الرقمية الجامعية هو أمر حيوي وضروري للحفاظ على سلامة وأمان البيانات والمعلومات الحساسة التي تتعامل بها المؤسسات التعليمية. ومن أجل ذلك، تتطلب هذه الخدمات تلبية عدد من المتطلبات الأساسية والمهمة، والتي يمكن تلخيصها كما يلي (زهودر، 2021) (بن قارة، 2021) (Matteo , Alessandro , & Riccardo , 2021) (Matthieu & Julien , 2023) (السمحان، 2020) (Avinash و Soyjaudah , 2014) (University

(Western Sydney (Chen, Luo, Shi, Cao, & Zhang, 2023) of Toronto, 2020)
:University, 2023)

10.1 المتطلبات الإدارية:

يجب على الجامعات وضع سياسات وإجراءات أمنية سليمة وتحديثها بشكل دوري لضمان مواكبة التهديدات الإلكترونية المتطورة. كما يتعين توفير برامج تدريبية وتوعوية دورية للموظفين والطلاب حول أساسيات الأمن السيبراني والمخاطر الأمنية المحتملة. بالإضافة إلى ذلك، يجب إنشاء فريق متخصص لإدارة الأمن السيبراني والتعامل مع حالات الاختراق بشكل فعال. ومن الضروري تحديد مسؤوليات الموظفين والطلاب فيما يتعلق بالأمن السيبراني وتزويدهم بالأدوات والإمكانيات اللازمة لأداء مهامهم بكفاءة. كما ينبغي تطبيق إجراءات تسجيل دخول آمنة، مثل المصادقة الثنائية، لحماية الأنظمة من الاختراقات. إلى جانب ذلك، يجب توفير إجراءات لحماية المعلومات الحساسة والملكية الفكرية، وتحديد سياسات واضحة لاستخدام الأجهزة الشخصية والتعامل مع المستخدمين المخالفين والمخترقين. وأخيراً، يجب تطبيق إجراءات النسخ الاحتياطي الدورية للبيانات وتقديم تقارير دورية لإدارة الجامعة حول حالة الأمن السيبراني وأي اختراقات محتملة.

10.2 المتطلبات التقنية:

يتطلب تعزيز الأمن السيبراني تحديث وتطوير الأنظمة الأمنية الحالية بشكل دوري لمواكبة التهديدات الجديدة. ويشمل ذلك توفير جدران حماية الشبكة وبرامج مكافحة الفيروسات والبرمجيات الخبيثة. كما يجب توفير نظام لتحليل السجلات ومراقبة الأنشطة لتتبع أي أنشطة غير مصرح بها أو اختراقات. بالإضافة إلى ذلك، ينبغي توفير خدمات استضافة مؤمنة ونسخ احتياطي للبيانات، وتطبيق إجراءات تأمين البرمجيات والتطبيقات الخاصة بالجامعة. كما يجب توفير خدمات التشفير والتوقيع الرقمي للبيانات، وإجراءات حماية من الهجمات المتعددة على مستوى الشبكات والتطبيقات. ولا بد من تطبيق اختبارات أمنية مستمرة لتحديد نقاط الضعف في الأنظمة الأمنية، وتأمين الاتصالات والشبكات اللاسلكية. وأخيراً، يجب توفير خدمات المراقبة والتحليل الأمني للأنظمة لضمان فعاليتها.

10.3 المتطلبات المادية:

لضمان أمن الخدمات الرقمية، يجب توفير الأجهزة اللازمة لتشغيل الأنظمة الأمنية بشكل فعال، مثل الخوادم والموجهات والجدران النارية. كما يتعين توفير البرامج والأدوات الأمنية اللازمة، مثل برامج مكافحة الفيروسات والحماية من البرمجيات الخبيثة. بالإضافة إلى ذلك، يجب توفير أجهزة أمنية متخصصة، مثل كاميرات المراقبة وأجهزة الكشف عن الحريق وأجهزة الإنذار. كما ينبغي توفير أجهزة لتأمين الشبكات اللاسلكية، مثل أجهزة التوجيه ونقاط الوصول اللاسلكية. ويجب تحديث الأجهزة المادية الحالية لضمان توافقها مع التقنيات الحديثة والمتطلبات الأمنية الجديدة. بالإضافة إلى ذلك، يجب توفير مراكز بيانات مؤمنة لتخزين البيانات والنسخ الاحتياطي، والأجهزة اللازمة لتنفيذ إجراءات الامتثال القانوني والتشريعي، مثل أجهزة التحليل الرقمي. وأخيراً، يجب توفير أجهزة متخصصة لتأمين الاتصالات والشبكات، مثل أجهزة تشفير البيانات وأجهزة التوجيه الآمنة.

10.4 المتطلبات البشرية:

يعد وجود فريق مختص بالأمن السيبراني أمراً ضرورياً لإدارة والإشراف على أمن الخدمات الرقمية. كما يجب توفير برامج تدريبية وتوعوية للمستخدمين حول الأمن السيبراني والمخاطر المحتملة. بالإضافة إلى ذلك، يتعين توظيف مهندسين ومتخصصين في تقنية المعلومات لإدارة وصيانة الأنظمة والتقنيات اللازمة. ويجب إنشاء فريق للحوادث والاستجابة الفورية للتعامل مع أي مشكلات تتعلق بالأمن السيبراني. كما ينبغي وجود فريق للمراجعة والتدقيق للتأكد من الامتثال لسياسات الأمن السيبراني والتشريعات المعمول بها.

10.5 المتطلبات القانونية والتشريعية:

يجب على الجامعات الامتثال للقوانين واللوائح الوطنية والدولية المتعلقة بالأمن السيبراني، مثل قانون حماية البيانات الشخصية واتفاقيات الأمم المتحدة ذات الصلة. كما يتعين توفير إجراءات للإبلاغ عن الاختراقات والتعامل معها وفقاً للقوانين المعمول بها. بالإضافة إلى ذلك، يجب تطبيق إجراءات لحماية السرية والخصوصية والمعلومات الحساسة والملكية الفكرية وفقاً للتشريعات ذات الصلة. كما ينبغي توفير خدمات التحقق

من الهوية والتوقيع الرقمي وفقاً للقوانين المنظمة لذلك. وأخيراً، يجب تطبيق إجراءات الاختبار الأمني والتأهيل الأمني وفقاً للمعايير الدولية. ومن بين المعايير الدولية التي يجب الالتزام بها:

- ✓ ISO 27001: معيار دولي يحدد أفضل الممارسات لإدارة أمن المعلومات.
- ✓ NIST Cybersecurity Framework: إطار عمل لإدارة الأمن السيبراني يتضمن معايير وممارسات أمنية موصى بها.
- ✓ PCI DSS: معيار يحدد متطلبات أمنية لحماية البيانات المالية.
- ✓ HIPAA: معيار يحدد متطلبات أمنية لحماية البيانات الصحية الشخصية.
- ✓ GDPR: لائحة تنظيمية لحماية البيانات الشخصية للمواطنين الأوروبيين، وتشمل متطلبات أمنية صارمة.

الإطار الميداني:

1. الخدمات الرقمية التي تقدمها جامعة المدينة:

تقدم جامعة المدينة العديد من الخدمات الرقمية للطلاب وأعضاء هيئة التدريس والموظفين والجمهور العام. ومن بين الخدمات التي تقدمها الجامعة عبر موقعها الإلكتروني (جمعة المدينة، 2023):

- البريد الإلكتروني الجامعي: توفر الجامعة بريداً إلكترونياً جامعياً لكل طالب وأستاذ وموظف
- خدمات استشارية وتوجيهية عن بعد: عبر منصة "انشغالات واقتراحات الأسرة الجامعية" لتقديم الدعم الأكاديمي والمهني للطلاب وأعضاء هيئة التدريس.
- نظام إدارة التعليم عن بعد عبر منصة التعليم عن بعد MOODLE
- المكتبة الرقمية الجامعية: لتقديم الدعم الأكاديمي والمهني للطلاب وأعضاء هيئة التدريس.

- نظام الإعلانات الجامعية والأخبار والمستجدات: للبقاء على إطلاع دائم بأحدث الأخبار والفعاليات الجامعية.
- قواعد بيانات إلكترونية: مثل المستودع رقمي جامعي DSpace، والذي يمكن من خلاله الوصول إلى الأبحاث والأطروحات الجامعية والمنشورات الأكاديمية الأخرى.
- الفهرس الآلي للمكتبات الجامعية (OPAC، PMB)
- فضاء الطالب USCOL : توفر منصة فضاء الطالب للطلبة الوصول إلى المواد الأكاديمية ومتابعة مسارهم الدراسي، من خلال حساب خاص بهم في هذه المنصة، يمكن الولوج اليه من موقع الجامعة. وتشمل هذه المنصة جملة من الخدمات البيداغوجية
- فضاء الأستاذ ESCOL: توفر منصة فضاء الأستاذ وسيلة للأساتذة لتتبع وإدارة العمليات الأكاديمية الخاصة بهم وصب نقاط الامتحانات وتقييم طلابهم وتقديم الملاحظات، حيث توفر هذه المنصة حساب خاص بكل أستاذ يمكن الولوج اليه من موقع الجامعة، وهذا حسب المقياس أو المقاييس المكلف بها
- الأرضية التقنية للحساب المكثف
- الإحالة إلى مواقع وقواعد بيانات وأرضيات رقمية ذات الصلة والأهمية للجُمهور: مثل التوثيق الإلكتروني SNDL، والمكتبة الرقمية اقرأ، مخبر البحث العلمي، مواقع الكليات، وزارة التعليم العالي والبحث العلمي، مركز البحث في الإعلام العلمي والتقني، الوكالة الجامعية للفرانكوفونية، البوابة الجزائرية للمجلات العلمية ASJP، بوابة البحث Researchgate، جوجل البحث العلمي وغيرها من المواقع وقواعد البيانات.
- خدمات تحميل الاستثمارات والوثائق: تتيح للطلاب وأعضاء هيئة التدريس والموظفين تحميل الاستثمارات والوثائق المطلوبة عبر الموقع الإلكتروني للجامعة.
- حاضنات جامعة المدينة: توفر الجامعة حاضنات تكنولوجية وريادية تدعم الابتكار وريادة الأعمال للطلاب وأعضاء هيئة التدريس والموظفين.
- مركز المساعدة النفسية جامعة المدينة عن بعد

- إصدارات الجامعة
- جداول التوقيت وجدول الامتحانات
- مقاطع فيديو جامعة المدينة: عبر منصة WEBTV ، تعرض محاضرات وندوات وفعاليات الجامعة عبر الإنترنت.
- دورات تدريبية عن بعد.
- خدمات التواصل الاجتماعي: تستخدم الجامعة وسائل التواصل الاجتماعي للتفاعل مع الطلاب وأعضاء هيئة التدريس والموظفين، وتوفير التحديثات والأخبار الجامعية والفعاليات القادمة.

2. السياسات والإجراءات الأمنية لحماية الخدمات الرقمية بجامعة المدينة:

تهدف جامعة المدينة إلى حماية خدماتها الرقمية من التهديدات الأمنية المحتملة من خلال وضع سياسات وإجراءات أمنية فعالة. وتتضمن هذه السياسات والإجراءات ما يلي:

2.1. ميثاق استخدام موارد الإعلام الآلي:

تم إعداد ميثاق استخدام موارد الإعلام الآلي من قبل جامعة المدينة، وهو متاح عبر [موقع الجامعة الإلكتروني](#). يهدف هذا الميثاق إلى وضع الأحكام والشروط اللازمة لاستخدام موارد الإعلام الآلي في الجامعة، بما في ذلك تحديد قواعد السلامة والاحتياطات التي يجب على المستخدمين احترامها. وتم الإمضاء والموافقة عليه من طرف جميع الموظفين بالجامعة من خلال حسابهم في منصة البروغرس PROGRES، ويتألف الميثاق من عشرة مواد وهي:

المقدمة

شرح مفاهيم نظم المعلومات والمصطلحات الأساسية المرتبطة بها لتوضيح مضمون الميثاق وأهدافه للمستخدمين.

المادة الأولى: الغرض من الميثاق

تحديد قواعد استخدام موارد الإعلام الآلي بالجامعة بشكل آمن ومسؤول من خلال إرشادات واضحة للمستخدمين.

المادة الثانية: نطاق التطبيق

الميثاق يسري على جميع المستخدمين داخل الجامعة وخارجها ممن يستعملون مواردها الرقمية والبريد الإلكتروني.

المادة الثالثة: الولوج إلى الموارد

تحديد سياسات الدخول للأمن للموارد الرقمية، مع التأكيد على المسؤولية، سرية المعلومات، وتوثيق الحسابات.

المادة الرابعة: سلامة أجهزة الكمبيوتر

توضيح إجراءات الحفاظ على سلامة الأجهزة من التلف والفيروسات، وضمان تهويتها وتحديثها بشكل منتظم.

المادة الخامسة: استخدام الإنترنت

تشدد على الاستخدام المسؤول للإنترنت، وتجنب المواقع الضارة أو غير اللائقة، وعدم تحميل ملفات مشبوهة.

المادة السادسة: البريد الإلكتروني الجامعي

استخدام البريد الجامعي بشكل آمن، دون مشاركة معلومات حساسة أو الرد على رسائل مشبوهة أو مجهولة.

المادة السابعة: منصة التعليم عن بعد

ضمان الاستخدام السليم للمنصة، مع الحفاظ على بيانات الدخول وتأكيد هوية المستخدمين والمشاركة الآمنة.

المادة الثامنة: النشر الإلكتروني بالجامعة

النشر على موقع الجامعة يجب أن يكون دقيقًا، محدثًا، ويُراعى فيه أمن المعلومات وصحة البيانات.

المادة التاسعة: مركز الحساب المكثف

تنظيم استخدام الباحثين للمركز عبر تحديد مساحة القرص، حذف الملفات المؤقتة، والتبليغ عن أي إساءة استخدام.

المادة العاشرة: التزام المستخدم

إلزام الجميع باحترام الميثاق، مع إمكانية فرض عقوبات عند المخالفة، وتسري الأحكام من تاريخ بدء العمل.

2.2. مركز الأنظمة وشبكات الإعلام والاتصال والتعلم المتلفز والتعلم عن بعد:

يعمل مركز الأنظمة وشبكات الإعلام والاتصال والتعلم المتلفز والتعلم عن بعد، التابع للمصالح المشتركة بجامعة المدينة على توفير الدعم اللازم للتعليم والتعلم عن بعد. ويتولى المركز مهام متعددة من بينها:

- استغلال وإدارة وتسيير البنية التحتية للشبكات.
- تطوير التطبيقات لخدمة وتسهيل التسيير البيداغوجي.
- متابعة تنفيذ مشاريع التعليم عن بعد والتعليم المتلفز.
- تقديم الدعم الفني لتصميم وإنتاج المقررات والدروس عبر الإنترنت.
- التكوين والإشراف على المشاركين في التعليم عن بعد.

2.3. مكتب الاستراتيجية الرقمية:

يعد مكتب الاستراتيجية الرقمية التابع لجامعة المدينة من الهيئات الرئيسية التي تتبع للجامعة، وقد تم تكليفه بمهام هامة تتعلق بالاستراتيجية الرقمية للجامعة وتطويرها. ومن بين المهام التي يقوم بها المكتب:

- وضع استراتيجية رقمية شاملة لتحسين جودة التعليم والبحث العلمي وتطوير الخدمات الإدارية والتواصل مع المجتمع.
- تطوير النظم الإلكترونية والتقنيات الحديثة لتحسين العمليات الأكاديمية والإدارية، وتوفير بيئة تعليمية حديثة ومتقدمة.
- تنسيق الجهود بين الأقسام والوحدات الأكاديمية والإدارية في الجامعة لتحقيق أهداف الاستراتيجية الرقمية.
- إدارة وتطوير مواقع الويب والتطبيقات الإلكترونية للجامعة والتأكد من توافقها مع المعايير الدولية.
- وفير التدريب والدعم الفني للطلاب والموظفين في استخدام التقنيات الحديثة والنظم الإلكترونية.

- العمل على تحسين مستوى الأمن السيبراني والحفاظ على سرية المعلومات وحمايتها من الاختراقات والاعتداءات الإلكترونية.
- البحث والتطوير في مجال التقنيات الحديثة وتطبيقاتها في العملية التعليمية والبحثية والإدارية.
- تكوين المستخدمين في مجال التكنولوجيا المعلومات

2.4. أنظمة وبرامج الحماية بجامعة المدية

لتحقيق أمن وسرية معلومات جامعة المدية، تستخدم الجامعة وحدة الحماية المتكاملة للمعلومات والشبكات، والتي تشمل البرامج التالية:

- برامج مكافحة الفيروسات: تستخدم للكشف عن الفيروسات والبرامج الضارة وإزالتها من الأجهزة المصابة. وهي مثبتة على جميع أجهزة الكمبيوتر بالجامعة.
- جدار الحماية (Firewall): يعمل على حماية الشبكة الداخلية للجامعة من هجمات القرصنة والمتسللين. يمكن لجدار الحماية أيضاً حجب المواقع غير الآمنة والمشبوهة.
- برامج مكافحة البريد العشوائي (Anti-spam): تستخدم لتصفية الرسائل الإلكترونية الواردة وإزالة البريد العشوائي والرسائل غير المرغوب فيها.

3. التحديات التي تواجه جامعة المدية لحماية خدماتها الرقمية (رحيم، 2023):

تواجه جامعة المدية العديد من التحديات والصعوبات في حماية خدماتها الرقمية، ومن أهم هذه التحديات:

- ندرة الخبرات والكوادر المؤهلة في مجال أمن المعلومات وحماية البيانات . خاصة في كليتها، حيث إن مجال أمن المعلومات يتطلب تأهيلاً وتدريباً مستمراً لمواكبة التهديدات المتزايدة.

- قلة الوعي بأهمية أمن المعلومات وسبل حماية البيانات لدى مستخدمي الخدمات الرقمية من طلبة وأعضاء هيئة تدريس وموظفين.
 - محدودية الموارد المالية المخصصة لحماية الخدمات الرقمية وتوفير البنية التحتية الأمنية اللازمة.
 - تعقيد البنية التحتية لتقنية المعلومات في الجامعة وكثرة نقاط الضعف التي يمكن استغلالها من قبل القرصنة والفيروسات.
 - صعوبة مواكبة التطور المذهل في أدوات ووسائل الهجوم الإلكتروني الحديثة.
 - محدودية التعاون وتبادل الخبرات بين الجامعات في مجال أمن المعلومات.
- كما أن جامعة المدينة مثل أي مؤسسة تعليمية أخرى، تواجه العديد من التحديات والصعوبات المشتركة وهي:
- ✓ التعقيد المتزايد للهجمات الإلكترونية. أصبحت الهجمات الإلكترونية معقدة بشكل متزايد، مما يجعل من الصعب على الجامعات حماية نفسها. يستخدم المهاجمون مجموعة متنوعة من التقنيات، بما في ذلك التصيد والبرامج الضارة وبرامج الفدية للوصول إلى أنظمة الجامعة وبياناتها.
 - ✓ العدد المتزايد للأجهزة المتصلة. يتزايد عدد الأجهزة المتصلة في الحرم الجامعي بسرعة، مما يزيد من صعوبة إدارتها وتأمينها. تشمل هذه الأجهزة أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية والأجهزة القابلة للارتداء.
 - ✓ الاستخدام المتزايد للحوسبة السحابية. تقوم العديد من الجامعات بنقل بنيتها التحتية لتكنولوجيا المعلومات إلى السحابة. قد يؤدي ذلك إلى زيادة صعوبة إدارة البيانات وتأمينها، حيث يتم تخزينها الآن على خوادم تابعة لجهات خارجية.
 - ✓ نقص مهارات الأمن السيبراني. هناك نقص في المتخصصين في الأمن السيبراني بالمهارات والخبرة اللازمة لحماية أنظمة الجامعة وبياناتها. هذا يجعل من الصعب على الجامعات العثور على أشخاص مؤهلين لشغل وظائف الأمن السيبراني.

✓ الأمن البشري: يتعلق هذا التحدي بالتهديدات الناجمة عن الأفراد الذين يعملون داخل الجامعة، والذين يمكنهم الوصول إلى المعلومات الحساسة والبيانات الشخصية للطلاب والموظفين، ويمكن أن يتسببوا في تسريب هذه المعلومات أو استخدامها بطرق غير مشروعة.

✓ التحديات القانونية والأخلاقية المتعلقة بحماية البيانات والخصوصية.

نتائج الدراسة:

توصلت الدراسة إلى النتائج التالية:

- تمتلك جامعة المدية خدمات رقمية متنوعة تخدم أهدافها التعليمية والبحثية والإدارية، يستخدمها طلابها وأعضاء هيئتها التعليمية والإدارية.
- تتبع جامعة المدية سياسات وإجراءات واضحة لحماية خدماتها الرقمية، مثل ميثاق استخدام موارد الإعلام الآلي
- تمتلك جامعة المدية مركز خاص بأنظمة المعلومات والتعلم والتعليم عن بعد، يقوم بتطوير وحماية الخدمات الرقمية، وكذلك مكتب الاستراتيجية الرقمية، يقوم بتحسين وتطوير قدرات الجامعة في مجال الخدمات الرقمية.
- تقوم الجامعة بتوعية موظفيها بأهمية الأمن السيبراني.
- تطبق جامعة المدية إجراءات أمنية فنية وإدارية لحفظ سلامة وسرية وصحة المعلومات الرقمية، مثل تحديث برامج الحماية وتنويعها، وصيانة الأجهزة التقنية، وإنشاء نظام شبكي آمن، وتوفير برامج حديثة للأمن السيبراني.
- تواجه جامعة المدية تحديات في تحقيق الأمن السيبراني بسبب محدودية الموارد المالية وتعقيد البنية التحتية لتقنية المعلومات وصعوبة مواكبة التطور المذهل في أدوات الهجوم الإلكتروني.

خاتمة:

حاولنا من خلال هذه الدراسة تسليط الضوء على السياسات والإجراءات الأمنية المتبعة لحماية الخدمات الرقمية في جامعة المدية، حيث تبين أن الجامعة تعتمد مجموعة

من الآليات التنظيمية والتقنية لضمان أمن معلوماتها الرقمية، رغم ما تواجهه من تحديات مرتبطة بالموارد البشري والمادي والتطور السريع في مجال الهجمات السيبرانية. كما أظهرت النتائج وجود هياكل تنظيمية مخصصة ومبادرات للتوعية والتحديث الأمني، مما يعكس وعياً بأهمية حماية البنية الرقمية. وتقتصر الدراسة في ختامها ضرورة تطوير السياسات الأمنية بشكل مستمر، وتكثيف التكوين والدعم التقني، مع إعادة هيكلة البنية التحتية، والاعتماد على المعايير الدولية. ومن المفيد أن تتجه الأبحاث المستقبلية نحو دراسة ثقافة الأمن السيبراني داخل الوسط الجامعي، ومدى فعالية التنسيق بين الجامعات الجزائرية في هذا المجال، إلى جانب إمكانية الاستفادة من النماذج العالمية الناجحة.

قائمة المراجع

- إنجي هند نجوى ريم سندس زهدور. (2021). استراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي. المجلة الدولية لنشر البحوث والدراسات، 214-252.
- جمعة المدينة. (08, 04, 2023). الصفحة الرئيسية. تم الاسترداد من موقع جامعة يحيى فارس بالمدينة/ <http://www.univ-medea.dz> :
- سليمان قطاف، و عبد الحليم بوقرين . (2022). الأمن السيبراني والمضامين المفاهيمية المرتبطة به. مجلة طبنجة للدراسات العلمية الأكاديمية، 37-56.
- عبد الوهاب احمد عبد الكريم، ومحمود عبد الرحمان خلف. (2020). اشكالية الأمن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات. مجلة دراسات السياسية.
- عبير أحمد علي كاعوه. (2020). سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية. مجلة دراسات تربوية واجتماعية، 134-200.
- فتيحة ليم، ونادية ليم. (2017). الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة. مجلة الفكر، 238-253.

محمد موسى مصطفى. (2003). أساليب إجرامية بالتقنية الرقمية: ماهيتها ... مكافحتها: دراسة مقارنة. القاهرة: مطابع الشرطة.

المركز الوطني للأمن السبراني. (05, 03, 2022). ما هو الأمن السبراني؟ تم الاسترداد من
المركز الوطني للأمن السبراني :
<https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html#>

مسعود رحيم. (15, 04, 2023). (الطاهر كباش، المحاور)

مصطفى إبراهيم سلمان الشمري. (2021). الأمن السبراني وأثره في الأمن الوطني العراقي. مجلة العلوم القانونية والسياسية، 149-190.

مصطفى عائشة بن قارة. (2021). استراتيجية تحقيق الأمن المعلوماتي للحكومة الالكترونية في الجزائر. المؤتمر الدولي الشامل للقضايا النظرية وسبل معالجتها العملية (الصفحات 25-37). دبي: دار الرافد للنشر.

منى عبد الله السمحان. (2020). متطلبات تحقيق الأمن السبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية-جامعة المنصورة، 1-29.

نجاحة حسين، وعبد القادر توزان. (2021). دور المكتبات الرقمية في خدمة البحث العلمي. جسر المعرفة، 337-348.

هيئة الحكومة الرقمية. (10, 04, 2023). دليل تعاريف المنصات والمنتجات والخدمات الرقمية. تم الاسترداد من هيئة الحكومة الرقمية :
https://www.dga.gov.sa/Definitions_Guide_of_Digital_Platforms_Products_and_Services

وزارة التعليم العالي والبحث العلمي. (04, 04, 2023). بروغرس. تم الاسترداد من mesrs: <https://www.mesrs.dz/index.php/progres-ar>

Abdulrahman, O., & Omar, I. M. (2018). The Impact of Applying Electronic ManagementSystem on the English Language Level: A Case study at

Cihan University. International Journal of Research and Engineering, 457-464.

Amazon Web Services. (2021, 03 01). Why data security is so important in the age of digital transformation. Retrieved from Times Higher Education: <https://www.timeshighereducation.com/hub/digital-innovation-higher-education/p/why-data-security-so-important-age-digital-transformation>

Bill , G., & Valerie , T. (2014). Building an Information Security Awareness Program Defending Against Social Engineering Hacks and Technical Threats. Published.

Bin Herzallah, M. (2021). E-Learning at the University of Algiers Reality and challenges. 91-74, *مجلة التعليم عن بعد والتعليم المفتوح*.

Catherine , C. (2023, 04 06). What is Third-Party Risk? Retrieved from UpGuard : <https://www.upguard.com/blog/what-is-third-party-risk>

Chachak, E. (2023, 04 03). Importance of Data Security in Higher Education Institutions. Retrieved from cyberdb: <https://www.cyberdb.co/importance-of-data-security-in-higher-education-institutions/>

Chen, H., Luo, X., Shi, L., Cao, Y., & Zhang, Y. (2023). Blockchain: Research and Applications. Beijing: Department of Computer Science, University of Science and Technology Beijing (USTB).

Ell, M., & Gallucci, R. (2022, 07 11). Educational institutions findings annex - Cyber Security Breaches Survey 2022 . Retrieved from GOV.UK :

<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022>

- Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge . Journal of Cyber Policy, 137-154.
- Hau Dicky . (2003). Unauthorized Access - Threats, Risk, and Control. Global Information Assurance Certification Paper ، 1-10.
- HurixDigital . (03 03, 2023). Importance of Data Security in Higher Ed Institutions for Data Protection . HurixDigital :
تم الاسترداد من :
<https://www.hurix.com/data-security-in-higher-ed-institutions/>
- Matar, H. (2020). Digital services: Concepts, challenges, and future directions. Information Technology & People, 1267-1289.
- Matteo , R., Alessandro , C., & Riccardo , R. (2021). An architecture to manage security operations for digital service chains. Future Generation Computer Systems, 252-266.
- Matthieu, J., & Julien , F. (2023). Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy. Computers in Human Behavior Reports, 1-8.
- Naidu, D., & Zainuddin, A. (2021). Cyber Security Threat Analysis in Higher Education Institutions during Covid-19 Pandemic. journal of syper security, 13-21.

Neetesh , S., Emma , H., Elisa , B., Patrick, O., Kim-Kwang, R., & Pete , B. (2020).
Impact and Key Challenges of Insider Threats on Organizations and
Critical Businesses. Electronics, 1-29.

Office of Information Security. (2023, 02 22). Information Security Policy.
Retrieved from the American University in Cairo:
<https://documents.aucegypt.edu/Docs/Policies/Information%20Security%20Policy.pdf>

Ramtohl Avinash و ، K.M.S. Soyjaudah. (2014). Information security
governance for e-services in southern African developing countries e-
Government projects. Journal of Science and Technology Policy
Management ،26-42.

University of Toronto. (2020, 03 02). Information Security and the Protection of
Digital Assets, Policy on [April 2, 2020]. Retrieved from University of
Toronto:
<https://governingcouncil.utoronto.ca/secretariat/policies/information-security-and-protection-digital-assets-policy-april-2-2020>

Western Sydney University. (2023, 04 05). Digital Information Security Policy.
Retrieved from Western Sydney University:
<https://policies.westernsydney.edu.au/view.current.php?id=00142>