جامعة غرداية

كلية العلوم الاقتصادية و التجارية وعلوم التسيير

قسم علوم التسيير

بالتعاون مع مخبر الدراسات التطبيقية في العلوم المالية والمحاسبة

ينظمون ملتقى وطني (حضوري/ عن بعد) بعنوان:

" مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي

للمؤسسات الاقتصادية"، يوم 04 ماي 2025.

مداخلة بعنوان:

دور التحول الرقمي في تعزيز الأمن السيبراني بالجامعة الجزائرية: التحديات والتدابير الوقائية دراسة حالة جامعة ادرار

من إعداد الباحثين :

- براهيم حاج عمر، أستاذ محاضر أ، جامعة غرداية، hadjamar.brahim@univ-ghardaia.edu.dz
-

من خلال المحور رقم: 2 .

الملخص: (لا يتجاوز 150 كلمة)

تهدف هذه الدراسة إلى تحليل دور التحول الرقمي في تعزيز الأمن السيبراني بالجامعة الجزائرية، مع التركيز على جامعة أدرار كنموذج تطبيقي. حيث تسلط الضوء على أهمية الإدارة الإلكترونية في تحسين الكفاءة وتقليل المخاطر الناتجة عن التعاملات الورقية، مع التركيز على التحديات الأمنية المرتبطة بها، وخاصة تهديدات الهندسة الاجتماعية مثل التصيد الاحتيالي وانتحال الشخصية، التي تستغل العامل البشري كأضعف حلقات المنظومة الأمنية.

تناولت الدراسة متطلبات التحول الرقمي الناجح، بدءًا من البنية التحتية التقنية ووصولًا إلى تدريب الموظفين على التوعية الأمنية

الكلمات المفتاحية:التحول الرقمي، الأمن السيبراني، الهندسة الاجتماعية، الإدارة الإلكترونية، التوعية الأمنية

Abstract:

This study aims to analyze the role of digital transformation in enhancing information security at Algerian universities, with a focus on the University of Adrar as a case study. It highlights the importance of electronic administration in improving efficiency and reducing risks associated with paper-based transactions, while emphasizing related security challenges - particularly social engineering threats such as phishing and identity theft that exploit human factors as the weakest link in security systems.

The study examines the requirements for successful digital transformation, ranging from technical infrastructure to employee training in security awareness.

Keywords: Digital transformation, Information security, social engineering, electronic administration, Security awareness.

.

1. مقدمة:

في ظل الثورة الرقمية المتسارعة التي يشهدها العالم المعاصر، تبرز إشكالية التحول الرقمي في المؤسسات الجامعية كتحدٍّ رئيسي يواجه القطاع التعليمي في الجزائر، ولا سيما في ظل تنامي التهديدات الأمنية المرتبطة بالفضاء السيبراني. تأتي هذه الدراسة لاستكشاف هذه الإشكالية من خلال التركيز على جامعة أدرار كنموذج تطبيقي، حيث تسعى إلى تحليل التحديات التي تواجه عملية الدمج بين متطلبات التحول الرقمي وضرورات الأمن المعلوماتي، في وقت لا تزال فيه العديد من المؤسسات الجامعية تعاني من ضعف البنى التحتية الرقمية وقصور الوعي الأمني بين منسوبيها.

تنبع أهمية هذه الدراسة من حاجتها الملحّة في المشهد الجامعي الجزائري الذي يشهد تحولات جذرية تفرضها متطلبات العصر الرقمي، حيث تهدف إلى تشخيص واقع البنية التحتية الرقمية، وتقييم مستوى الجاهزية الأمنية، وصولاً إلى اقتراح إطار عمل متكامل يحقق التوازن بين متطلبات الرقمنة وضمانات الحماية السيبرانية.

تستند الدراسة إلى مجموعة من الفرضيات الرئيسية التي تؤكد وجود علاقة طردية بين جودة البنية التحتية ومستوى الأمن المعلوماتي، كما تفترض أن ارتفاع مستوى الوعي الأمني يسهم بشكل مباشر في تعزيز فاعلية أنظمة الحماية، في حين أن الإجراءات الإدارية التقليدية تشكل عائقاً أمام التحول الرقمي الفعّال. كما تذهب الدراسة إلى افتراض أن تطبيق معايير الأمن المعلوماتي يمكن أن يقلل من مخاطر الاختراقات بنسبة كبيرة.

تكمن الإشكالية المركزية للدراسة في محاولتها الإجابة عن السؤال الجوهري: كيف يمكن تحقيق التكامل بين متطلبات التحول الرقمي المتسارع وضرورات الأمن المعلوماتي في البيئة الجامعية الجزائرية؟ هذا السؤال الذي يتفرع بدوره إلى عدة تساؤلات فرعية تتعلق بمدى جاهزية البنى التحتية، وأثر الثقافة التنظيمية، وطبيعة التهديدات السيبرانية التي تواجهها المؤسسات الجامعية في ظل التحولات الرقمية الحالية.

اعتمدت هذه الدراسة المنهج الوصفي التحليلي كإطار منهجي رئيسي، حيث يتميز هذا المنهج بقدرته على دراسة الظواهر في سياقها الطبيعي ووصفها بدقة عبر الجمع بين التحليل الكيفي والكمي. وقد تم اختيار هذا المنهج لملاءمته لطبيعة الدراسة التي تسعى إلى تشخيص واقع التحول الرقمي والأمن المعلوماتي في البيئة الجامعية، مع التركيز على الجوانب التالية:
الوصف الكيفي: تحليل الخصائص النوعية للظاهرة والتحليل الكمي: قياس الجوانب القابلة للتكميم

أدوات جمع البيانات: تم الاعتماد على الاستبيان كأداة رئيسية لجمع البيانات، حيث تم تصميمه وفق المعايير التالية: تضمن ثلاثة محاور رئيسية (البنية التحتية، الممارسات الرقمية، الوعي الأمني) طبق على عينة ممثلة من منسوبي الجامعة (أعضاء هيئة تدريس، إداريين، طلاب)

2. مفاهيم ومصطلحات الدراسة

1.2 الإدارة:

هي مصدر أدار يدير ادارة، تقول العرب: أدرت الشيء أديره ادارة، وأدار[1] الشيء يديره ادارة، ويريدون من ذلك التعدي التدوير للشيء دورانا ذات اليمين وذات الشمال. في حين يعرفها علماء الاجتماع مثال تايلور بأنها: التحديد الدقيق لما يجب على الأفراد عمله، ثم التأكد[2]

2.2 الإدارة الالكترونية:

هي استغلال الادارة لتكنولوجيات المعلومات والاتصالات لتمكن من تسهيل العمليات وتطويرها داخل المنظمات.[3] ويمكن القول بأنها تلك العمليات الادارية التي تستخدم من خلالها مختلف الوسائل والتجهيزات التكنولوجية المتطورة لتسهيل العملية التنظيمية داخل المنظمة، مع جهد أقل وتكلفة معقولة.

3.2 الأمن السيبراني:

جميع الإجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، ويشمل كذلك حماية الأجهزة والبيانات.

4.2 التحول الرقمي:

عملية استراتيجية شاملة تعتمد على دمج التقنيات الرقمية في جميع جوانب العمل المؤسسي، بهدف إحداث تحسين جذري في آليات الأداء وخلق قيمة مضافة"[4]

5.2 الأمن المعلوماتي:

حماية البيانات والنظم المعلوماتية من الوصول غير المصرح به، أو التعديل، أو التعطيل، عبر تطبيق سياسات تقنية وإدارية متكاملة"[5]

---

[11] نايف شعبان، عبد الله قرموط. "الادارة في سورة يوسف عليه السلام" رسالة لاستكمال متطلبات الحصول على درجة الماجستير في التفسير وعلوم القرءان. الجامعة الاسلامية (غير منشورة). غزة، 2009م.ص31.

[2] طلعت، ابراهيم لطفي. "علم اجتماع التنظيم" القاهرة، دار غريب للطباعة والنشر والتوزيع, 2007م، ص56.

[3] فداء، حامد. "الادارة الالكترونية الأسس النظرية والتطبيقية" الأردن: دار مكتبة الكندي, 2015م، ص203.

[4] صالح، خالد التحول الرقمي في المؤسسات العربية. دار العلم، القاهرة2022، ص 45.

[4] OECD (2021). Cybersecurity Guidelines for Public Sector. Paris: OECD Publishing. p.23.

[4] **https ab7as : net.**

3. أهداف الأمن السيبراني: [6]

-تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
-التصدي لهجمات وحوادث امن المعلومات التي تستهدف المؤسسات القطاع العام والخاص.
-توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.
- صمود البني التحتية الحساسة للهجمات الإلكترونية.
- توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
-سد الثغرات في أنظمة امن المعلومات.
- مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين.
- حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات ت الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

4. أهمية الأمن السيبراني:

في عالم اليوم المترابط بواسطة الشبكات، يستفيد الجميع من برامج الدفاع السيبراني.
وتتمثل أهمية الأمن السيبراني فيما يلي:
- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها
- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها
- حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.

5. تحليل البيانات المتعلقة بالدراسة:

الجدول (01): يمثل توزيع الاستمارات الموزعة

الاستمارات الموزعة	المسترجعة	القابلة للدراسة	المجموع	النسبة المئوية
110	96	63	63	57

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

الجدول (02): يمثل توزيع عينة الدراسة حسب الجنس في المؤسسة محل الدراسة

البيان	التكرار	النسبة المئوية
ذكر	41	65
أنثى	22	34
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

يتبين من خلال الجدول رقم (01) أن الفئة الغالبة على العينة هي فئة الذكور حيث تمثل 41وتقدر بنسبة % 65 من اجمالي العينة، بينما تمثل نسبة %34بتكرار 22المتبقية نسبة الاناث من هذه العينة، وهي نسبة صغيرة بالنسبة للذكور.
يمكن تفسير ذلك من خلال طبيعة الوظيفة الادارية التي يشغلها غالبا الذكور، دون غض النظر عن طبيعة المجتمع الذي طبقت فيه الدراسة بمنطقة أدرار، حيث يعرف على هذا المجتمع أنه مجتمع محافظ والمجتمعات المحافظة يقل فيه دفع النساء الى التوظيف خاصة في الادارات والمصالح التي تشهد اقبال كبير من المتعاملين.

الجدول (03): يمثل توزيع عينة الدراسة حسب المستوى التعليمي في المؤسسة محل الدراسة

البيان	التكرار	النسبة المئوية
ثانوي	2	3
ليسانس	12	19
دكتوراه	49	77
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

يتبين من الجدول رقم (03) أن المستوى التعليمي الغالب على هذه العينة هو المستوى دكتوراه بتكرار49 ونسبة تقدر ب:77%، ثم تليها نسبة المستوى ليسانس التي تقدر ب:19% بتكرار 12من اجمالي العينة، في حين مستوى الثانوي يمثل أقل عدد بتكرار 2 ونسبة تقدر ب 3% من اجمالي عينة الدراسة.
ويمكن تفسير ذلك من خلال أن مؤسسة الجامعية تعتمد في توظيفها على أساس المؤهلات العلمية خصوصا الجامعيين، من أجل رفع كفاءتهم، ولأنها تعتمد على الانتاج المعرفي هذا ما ألزمها استقطاب فئات ذوي مستوى عال.

الجدول (04): يمثل توزيع عينة الدراسة حسب سنوات خبرة في المؤسسة محل الدراسة

البيان	التكرار	النسبة المئوية
أقل من سنة	5	7
أكثر من 5 سنوات	30	47
10سنوات	6	9
10اكثر من سنوات	22	34
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

يتبين من خلال الجدول رقم **(04)** أن العاملين الذين لديهم خبرة أكثر من 10 سنوات يمثلون النسبة الأكبر بتكرار 47 وبنسبة تقدر ب: 47% ما يقارب النصف من اجمالي العينة، ثم تليها فئة العاملين الذين لديهم أكثر من 5 سنوات خبرة بتكرار 22 وبنسبة تقدر ب: 34%، ثم تليها نسبة العاملين الذين لديهم 5 سنوات خبرة

يمكن تفسر ذلك بأن أغلب الموظفين هم من فئة الشباب وبالتالي يتم نقل خبراتهم بين الموظفين، ومع الاستحداثات المستمرة للمؤسسة يستدعي توظيف خبرات جديدة لمواكبة تلك الاستحداثات.

6. تحليل البيانات المتعلقة بالأمن السيبراني:

الجدول رقم (05) يوضح مدى تواجد بالجامعة أنظمة حماية للأجهزة

	التكرارات	النسبة
نعم	55	87,3
لا	8	12,7
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

يتبين من خلال الجدول نلاحظ أن المؤسسة توفر انظمة حماية الأجهزة وهذا حسب نسبة المجيبين بنعم وتقدر نسبتهم ب 87.3% بتكرار 55 من اجمالي العينة بينما المجيبين بلا تقدر نسبتهم ب 12.7% بتكرار 8 من اجمالي العينة.

ويفسر ذلك أن توجه الجامعة بشكل خاص لاقتناء التجهيزات من جهة وكذا نتيجة لطبيعة عمل المؤسسة حيث تعتمد بنسبة كبيرة على الأجهزة الالية والرقمية.

الجدول رقم (05) يوضح قيام المؤسسة بتحديث الأجهزة القديمة؟

	التكرار	النسبة
نعم	35	55,6
لا	3	4,8
أحيانا	25	39,7
المجموع	63	63

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

نلاحظ من خلال الجدول أن 55.6% من عينة الدراسة ترى أن المؤسسة تقوم بتحديث الأجهزة القديمة، بينما نلاحظ 39.7% من عينة الدراسة ترى أنه أحيانا ما تقوم المؤسسة بتحديث أجهزتها.
يمكننا تفسير نسبة المجيبين بنعم بأن المؤسسة تسعى لمواكبة التغيرات والتحديثات المستمرة على مستوى الاعلام الآلي والأجهزة الالكترونية لكي تتجنب العجز، أما المجيبين ب أحيانا والتي تعد نسبتهم معتبرة من عينة الدراسة يفسر هذا بأن تحديث الأجهزة القديمة يكون حسب ما تخصصه الجهة الوصية من الميزانية العامة وبما أنه كانت هاته الدراسة في ظل جائحة كورونا، فعلى أثرها شهدت المؤسسات عجزا اقتصاديا واضحا ما قد يجعلها تأجل أو تلغي بعض الأغلفة المالية الخاصة بتحديث الأجهزة.

الجدول رقم (06) يوضح تحديث برامج الحماية لأجهزة الحاسب الآلي للجامعة.

	التكرارت	النسبة
نعم	58	92,1
لا	5	7,9
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

نلاحظ من خلال الجدول أن 92.4% من عينة الدراسة ترى أنه توجد تحديث لبرامج حماية في حين يرى 7.9% من عينة الدراسة أنه لا تتوفر تحديث للبرامج المؤسسة بفروعها.

الجدول رقم (07) يوضح مدى توجد أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالجامعة

البيان	التكرار	النسبة المئوية
لا	59	93,7
نعم	4	6,3
محايد	/	/

المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول نلاحظ أن 93.7% من عينة الدراسة ترى أن انظمة حماية الأجهزة الالكترونية غير موجودة، ونلاحظ نسبة قليلة تقدر ب 6.3% من عينة الدراسة ترى أن انظمة حماية الاجهزة الالكترونية موجودة.
ويفسر ذلك أن درجة الانجاز العمل مرهون بمدى توفر انظمة حماية الأجهزة الالكترونية، حيث تشهد المؤسسة تقدما ملحوظا في استخدام الأجهزة الحديثة والاعتماد عليها بشكل كبير أي أنه أصبحت تضخ ميزانيات كبرى لذلك.

الجدول رقم (08) يوضح مدى تزيد الادارة الالكترونية من الكفاءة والفعالية المطلوبة في اداء المهام؟

البيان	التكرار	النسبة المئوية
نعم	56	88,9
لا	7	11,1
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول اعلاه نلاحظ ان نسبة 88,9من افراد العينة يؤكدون ان الادارة الالكترونية تعمل على تطوير الدائم للموظفين لأدائهم باستمرار، ان نسبة 11,1من افراد العينة لا يرون ان الادارة الالكترونية لا تساعد على تطوير الموظفين لأدائهم ويفسر ذألك بان الادارة الالكترونية تعمل تحيين وتجديد المعلومات للأفراد من خلال التطور العامل للمعلومة والتكنولوجيا والتقنية الجديدة.

الجدول رقم (09) يوضح مدى تطبق متطلبات الامن السيبراني لإدارة هويات الدخول والصلاحيات

البيان	التكرار	النسبة المئوية
نعم	59	93,7
لا	3	4,8
محايد	1	1,6
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول نلاحظ 93.7% من عينة الدراسة ترى الادارة الالكترونية تقلل من الأخطاء المهنية أثناء العمل، وترى نسبة 4.8% من عينة الدراسة ترى أن الادارة الالكترونية لا تقلل من الأخطاء المهنية أثناء العمل، بينما 1.6% من عينة الدراسة اجابوا ب أحيانا. ويفسر ذلك أن مؤسسة باعتمادها الادارة الالكترونية قللت من الأخطاء المهنية التي كانت ترتكب في الادارة التقليدية، وهذا ما يعمل على تحسين أداء العاملين وكذا تحسين الخدمة

الجدول رقم (10) يوضح مدى تطبق متطلبات الامن السيبراني لحماية أنظمة المعلومات الإدارية ومعالجة أجهزة المعلومات بالجامعة

البيان	التكرار	النسبة المئوية
نعم	62	98,4
لا	1	1,6
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول نلاحظ ان نسبة 98,4من افراد العينة يؤكدون ان **تطبق متطلبات الامن السيبراني لحماية أنظمة المعلومات الإدارية ومعالجة أجهزة المعلومات بالجامعة** يساعد في اتخاذ القرارات السليمة وفي الاوقات المناسبة ونسبة 1,6 من افراد العينة لا يوافقون فكرة ان الادارة الالكترونية لا تساعد في اتخاذ القرارات السليمة في الاوقات المناسبة، ويفسر ذلك ان الادارة الالكترونية لدى مؤسسة تساهم في اتخاذ القرارات السليمة وفي الاوقات المناسبة مما يعمل على تحسين اداء العاملين في تأدية الخدمة العمومية.

الجدول رقم (11) يوضح مدى توفر الجامعة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة الجامعة؟

البيان	التكرار	النسبة المئوية
نعم	58	92,1
لا	5	7,9
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول اعلاه نلاحظ ان92/من افراد العينة ترى ان **توفر الجامعة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة الجامعة** تعمل على تحسين وتحديث المعلومات والبيانات اللازمة للأداء الاعمال بينما ترى نسبة, 7.9/ من افراد العينة انها لا تساعد على تحديت وتحسين البيانات الازمة لأداء الاعمال ,يفسر ذلك ان **برامج حماية** الادارة الالكترونية في مضمونها والياتها تعمل على تحسين وتحديث البيانات والمعلومات الازمة لأداء الاعمال الادارية والخدمة العمومية وهو ما يتماشى مع التطورات الحاصلة في جميع المجالات الذي يتطلب السرعة والدقة في اداء الاعمال

الجدول رقم (12) يوضح تطبق متطلبات الأمن السيبراني إدارةالأصول المعلوماتية والتقنية بالجامعة

البيان	التكرار	النسبة المئوية

نعم	61	96,8
لا	2	3,2
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول اعلاه نلاحظ ان نسبة 96,8من افراد العينة يؤكدون ان **متطلبات الأمن السيبراني في إدارة الأصول المعلوماتية والتقنية بالجامعة** الادارة الالكترونية تعمل على تقييد العاملين بالإجراءات وقواعد العمل المنصوص عليها في تشريعات العمل واللوائح التنظيمية بينما ترى نسبة 3,2 انها لا تسعد على التقيد بقواعد العمل، مما يفسر دلك ان الادارة الالكترونية تعمل على احترام قواعد العمل وإجراءاته مما يجعل العامل في اريحية امام المهام الموكل له من خلال وضوح الادوار والوظائف والحدود الفاصلة بين كل دور واخر

الجدول رقم (13) يوضح مدى تطبق الجامعة متطلبات الأ من السيبراني لحماية البريد الالكتروني

البيان	التكرار	النسبة المئوية
نعم	56	88,9
لا	7	11,1
محايد	/	/
المجموع	63	100,0

المصدر: من إعداد الباحث بالاعتماد على مخرجاتspss

من خلال الجدول اعلاه نلاحظ ان نسبة 88,9من افراد العينة يؤكدون ان **متطلبات الأمن السيبراني لحماية البريد الالكتروني ضرورية** للإدارة الالكترونية تعمل على تطوير الدائم للموظفين لأدائهم باستمرار، ان نسبة 11,1من افراد العينة لا يرون انها لا تساعد على تطوير الموظفين لأدائهم ويفسر ذلك بانها تعمل تحيين وتجديد المعلومات للأفراد من خلال التطور العامل للمعلومة والتكنولوجيا والتقنية الجديدة.

الجدول رقم 14 يوضح العلاقة بين تحديث الأجهزة القديمة وبقاءها صالحة لمدى بعيد.

تحديث الاجهزة / الاجهزة صالحة لمدى بعيد		نعم	لا	المجموع
نعم	التكرار	25	10	35
	%النسبة المئوية	39.7%	15.9%	55.6%
لا	التكرار	3	0	3

	%النسبة المئوية	4.8%	0.0%	4.8%
أحيانا	التكرار	24	1	25
	%النسبة المئوية	38.1%	1.6%	39.7%
المجموع	التكرار	52	11	63
	%النسبة المئوية	82.5%	17.5%	100.0%

المصدر: مخرجات spss

من خلال الجدول يتبين أن 82.5% من المبحوثين أكدوا أن المؤسسة تقوم بتحديث الأجهزة القديمة منهم 39.7% أكدوا أن ذلك يعمل على بقاء الأجهزة صالحة لمدى بعيد كذا 38.1% أكدوا أنه أحيانا ما يكون ذلك في حين 4.8% يروا عكس ذلك، فيما نجد 17.5% أكدوا أن المؤسسة لا تقوم بتحديث الاجهزة القديمة منهم 15.9% أكدوا أن هاته الوضعية تعمل على ابقاء الاجهزة صالحة لمدى بعيد في حين 1.6% أكدوا أنه أحيانا ما يكون ذلك.

من خلال النسب يتأكد لنا أن مؤسسة الوحدة البريدية لولاية أدرار تخصص ميزانية معتبرة لتحديث الاجهزة ما يجعلها صالحة لمدى بعيد وقد يكون ذلك أحيانا نظرا للتحديث المستمر للأجهزة مما لا يجعل هناك داعيا لتحديثها مرة أخرى

7. نتائج الدراسة:

من خلال جمع المعطيات من المجتمع الإحصائي وتحليلها واختبار فرضيات الدراسة تمكنا من الخروج بنتائج هذه الدراسة.

- يتضح لنا من خلال الدراسة أن مؤسسة جامعية تساهم بشكل فعال في تطبيق الإدارة الالكترونية لتحسين الأداء والحماية للعاملين، فقد أوضحت النتائج أن مؤسسة توفر عددا كافيا من الأجهزة الالكترونية.
- معظم العاملين بالمؤسسة الجامعية يمتلكون البريد **الالكتروني** مهني مما يسهم في تواصل العاملين بالوحدات الأخرى عن طريق الشبكة الرقمية ما يضمن التنسيق المستمر بين الفروع وكذا ضمان وضوح المعاملات.
- ان مؤسسة الجامعية لا تقوم بالتدريب الكافي للعاملين على الأجهزة الالية
- اتقان العمل في مؤسسة الجامعية مرهون بمدى توفر الأجهزة الالكترونية، حيث تشهد المؤسسة تقدما ملحوظا في استخدام الأجهزة الحديثة والاعتماد عليها بشكل كبير.
- مؤسسة الجامعية باعتمادها الادارة الالكترونية قللت من الأخطاء المهنية التي كانت ترتكب في الادارة التقليدية، وهذا ما يعمل على تحسين أداء العاملين وكذا تحسين الخدمة.
- ان الادارة الالكترونية لدى مؤسسة جامعية تساهم في اتخاذ القرارات السليمة وفي الاوقات المناسبة مما يعمل على تحسين اداء العاملين في تأدية الخدمة العمومية.

-التغير المتمثل في سوء استخدام الادارة الالكترونية أدى الى عدم وجود علاقة بينها وبين الاداء الوظيفي

8. خاتمة:

سعت دراستنا الموسومة بـ **"دور التحول الرقمي في تعزيز الأمن السيبراني بالجامعة الجزائرية: التحديات والتدابير الوقائية "**إلى تحليل أهمية الإدارة الإلكترونية في المؤسسات الجامعية، مع التركيز على جامعة أدرار كنموذج تطبيقي. وهدفت الدراسة إلى تقييم مدى جاهزية المؤسسة للتحول الرقمي في ظل التحديات الأمنية الناشئة، لا سيما **مخاطر الهندسة الاجتماعية** التي تستغل العامل البشري كأحد أضعف الحلقات في منظومة الأمن السيبراني.

تمثلت أهداف الدراسة في:

1. الكشف عن مدى وعي العاملين بمخاطر **الهندسة الاجتماعية** (مثل التصيد الاحتيالي وانتحال الشخصية) وانعكاساتها على أمن البيانات.
2. تقييم ضرورة تبني الإدارة الإلكترونية لمواكبة عصر التكنولوجيا، عبر توفير معلومات دقيقة مع تقليل الثغرات الناجمة عن التعاملات الورقية.
3. تحليل متطلبات التحول الرقمي، بدءًا من البنية التحتية ووصولًا إلى تدريب الموظفين على **التوعية الأمنية** لمواجهة تهديدات الهندسة الاجتماعية.

كما أبرزت الدراسة أن ضعف الوعي بمخاطر **التلاعب النفسي** (كجزء من الهجمات الاجتماعية) قد يُعيق تطبيق الإدارة الإلكترونية، مما يستدعي إدماج استراتيجيات أمنية شاملة، مثل:

- اعتماد أنظمة مصادقة متعددة العوامل.
- تنظيم حملات توعوية دورية للعاملين حول **حماية الهوية الرقمية**.
- تطوير سياسات واضحة للإبلاغ عن المحاولات المشبوهة.

وفي الختام، أكدت الدراسة على أن نجاح التحول الرقمي في الجامعة الجزائرية مرهون بموازنة بين التطوير التقني و**تعزيز الثقافة الأمنية**، خاصة في بيئة تزداد فيها الهجمات المعتمدة على التلاعب البشري.

توصيات البحث:

- التأكيد على ضرورة اهتمام جامعة بمتطلبات حماية أنظمة المعلومات الادارية بالجامعة.
- إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في البرامج المدرسة.
- تشجيع بحوث ودراسات الأمن السيبراني في أطروحات الماجستير والدكتوراه
- تشجيع مجالات البحث العلمي والابتكار في مجال الأمن السيبراني
- توعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرساء بنية تحتية للدخول إلى مجال صناعة البرمجيات العالمية والقدرة علي منافسة المنتج المستورد
- تشجيع مؤسسات المجتمع المدني والتأكيد على دورها الفعال في التعامل مع الاستخدام م غير الآمن لتكنولوجيا المعلومات، وذلك من خلال الأنشطة العلمية ونشر ثقافة الاستخدام الآمن لشبكة الانترنت والتطبيقات الرقمية الحديثة.
- تشجيع الاستثمار في مجال الأمن السيبراني وينقسم الاستثمار لجانبين، الأول توطين.

التكنولوجيا والبني التحتية السيبرانية، الثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.

- اجراء مزيد من الدراسات العلمية حول قضية أمن المعلومات بمختلف مؤسسات عامة، ومجال التعليم بشكل خاص.
- عقد دورات تدريبية مستمرة للعاملين في مجال المعلومات.

9. قائمة المراجع:

- نايف شعبان، عبد الله قرموط. "الادارة في سورة يوسف عليه السلام" رسالة لاستكمال متطلبات الحصول على درجة الماجستير في التفسير وعلوم القرءان. الجامعة الاسلامية (غير منشورة). غزة، 2009م.ص31.

طلعت، ابراهيم لطفي. "علم اجتماع التنظيم" القاهرة، دار غريب للطباعة والنشر والتوزيع, 2007م، ص56.

فداء، حامد. "الادارة الالكترونية الأسس النظرية والتطبيقية" الأردن: دار مكتبة الكندي, 2015م، ص203.

صالح، خالد التحول الرقمي في المؤسسات العربية. دار العلم، القاهرة2022، ص 45.

OECD (2021). Cybersecurity Guidelines for Public Sector. Paris: OECD Publishing. p.23.

//https ab7as :net.