**جامعة غرداية**

**كلية العلوم الاقتصادية و التجارية وعلوم التسيير**

**قسم:علوم التسيير**

**مذكرة التخرج لنيل شهادة ليسانس أكاديمي**

**في ميدان: العلوم الاقتصادية والتجارية وعلوم التسيير**

**شعبة: علوم التسيير**

**تخصص : إدارة الاعمال**

**بموضوع** :

**أمن نظم المعلومات في المؤسسات الخدمية**

**دراسة حالة \_ مديرية بريد الجزائر وحدة غرداية**

**من اعداد الطلبة : تحت اشراف الأستاذة :**

* **العنق أيوب د.عجيلة حنان**
* **الشقمة منير**
* **حميد اوجانة احمد**

**نوقشت واجيزت علنا بتاريخ 16/06/2025**

**أمام اللجنة المكونة من السادة :**

**.د/ بلعربي محمد جامعة غرداية رئيسا**

**.د/ عجيلة حنان جامعة غرداية مشرفا ومقررا**

**.د/ بباز عبد العزيز جامعة غرداية مناقشا**

**الموسم الجامعي:2025/2024**

**جامعة غرداية**

**كلية العلوم الاقتصادية و التجارية وعلوم التسيير**

**قسم علوم التسيير**

**مذكرة التخرج لنيل شهادة ليسانس أكاديمي**

**في ميدان: العلوم الاقتصادية والتجارية وعلوم التسيير**

**شعبة: علوم التسيير**

**تخصص : إدارة الاعمال**

**بموضوع** :

**أمن نظم المعلومات في المؤسسات الخدمية**

**دراسة حالة \_ مديرية بريد الجزائر وحدة غرداية**

**من اعداد الطلبة : تحت اشراف الأستاذة :**

* **العنق أيوب د.عجيلة حنان**
* **الشقمة منير**
* **حميد اوجانة احمد**

**نوقشت واجيزت علنا بتاريخ 16/06/2025**

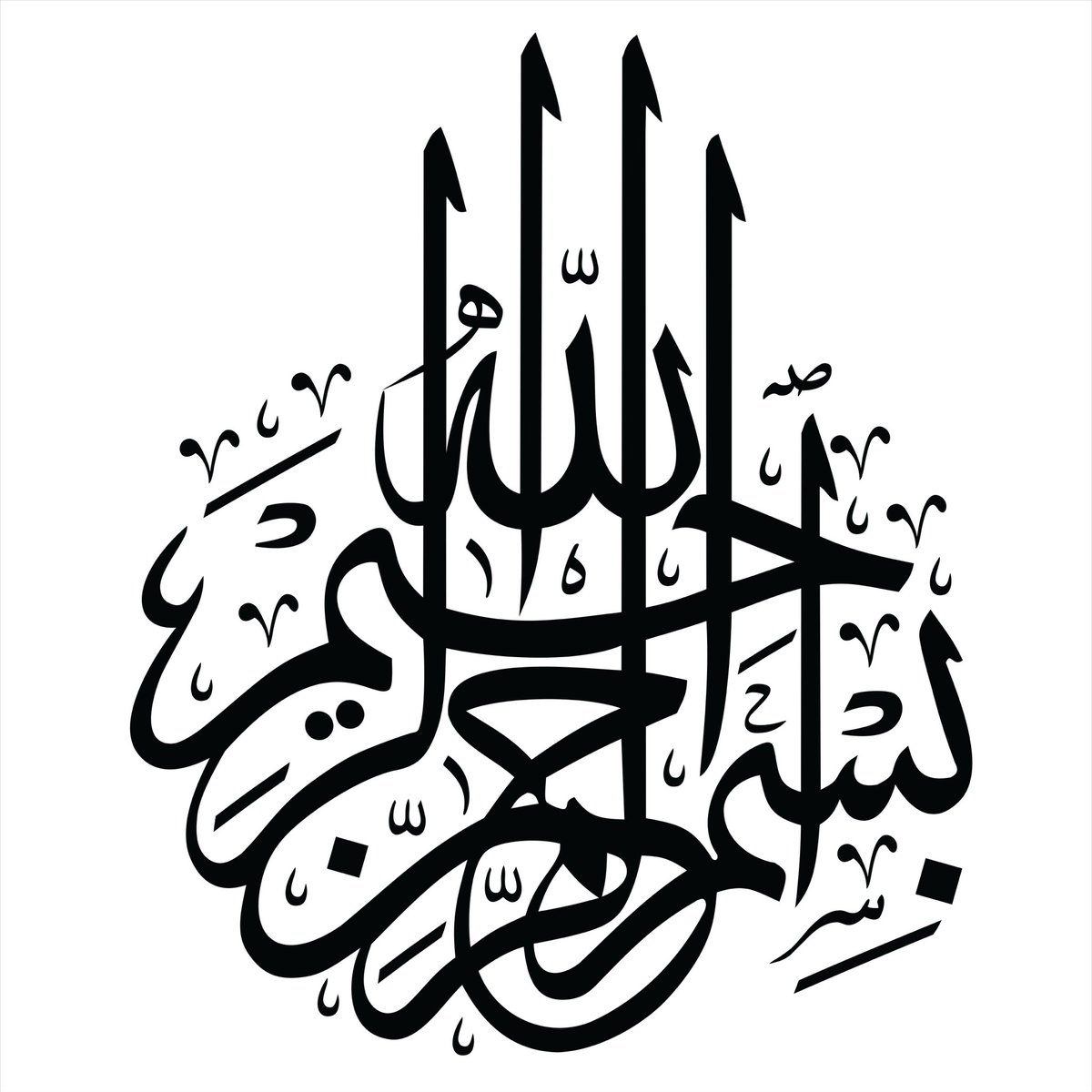
**أمام اللجنة المكونة من السادة :**

**.د/ بلعربي محمد جامعة غرداية رئيسا**

**.د/ عجيلة حنان جامعة غرداية مشرفا ومقررا**

**.د/ بباز عبد العزيز جامعة غرداية مناقشا**

**الموسم الجامعي:2025/2024**



**بًسِمً آلَلَهّ آلَرحًمًنِ آلَرحًيَمً**

(قُلَ هّلَ يَسِتٌوٌيَ آلَذِيَنِ يَعٌلَنِوٌنِ وٌآلَذِيَنِ لَآيَعٌلَمًوٌنِ إنِمًآ يَتٌذِکْر آوٌلَوٌ آلَآلَبًآبً)

سورة الزمر الاية "9"

**صّدٍقُ آلَلَهّ آلَعٌظُيَمً**

**الاهداء**

**أهدي هذا العمل**

**إلى نفسي التي تحملت التعب، واجتهدت رغم الصعوبات، وآمنت بأن لكل مجتهد نصيب**

**إلى والديّ العزيزين، سندي في هذه الحياة، نبض دعواتهم كان النور الذي أنار طريقي**

**إلى إخوتي، شركاء الفرح، ومصدر الدعم والتشجيع الدائم**

**أهدي هذا الإنجاز المتواضع، تعبيرًا عن حبي وإمتناني**

**الشقمة منير**

**الاهداء**

**و آخِرُ دَعْوَاهُم أَنِ الحَمْدُ لِلَّهِ رَبِّ العَالَمِينَ " الحمد لله عند البدء و عند الختام، من قال أنا لها نالها**

**لقد كانت طريقا طويلة مليئة بالإخفاقات والنجاحات فخورين بكفاحنا لتحقيق أحلامنا**

**لحظة لطالما انتظرتها وحلمت بها في حكاية اكتملت فصولها**

**أهدي ثمرة جهدي هذه إلى من أوصاني بهما الله برا وإحسانا والدي الكريمين، أطال الله في عمرهما، وألبسهما لباس الصحة والعافية**

**إلى من جمعنا معهم بيت واحد وكانوا خير سند اخوتي الأعزاء كل باسمه**

**إلى رفقاء الدرب من غادرونا وبقيت كلماتهم وقعا في آذاننا**

**إلى من علمني حرفا طيلة مساري الدراسي ولم يبخل بعطاءه، أساتذتي الأفاضل كل باسمه ومقامه**

**إلى نفسي التي راهنت على النجاح، اصبري وصابري فلا يزال الطريق طويل**

**وإلى كل من اتسع قلبي لهم وضاقت هذه الورقة عن ذكرهم، أهديكم عملي المتواضع عرفانا لكم بالجميل، وتقديرا لجهودكم**

**العنق أيوب**

**الاهداء**

**لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون ، لم يكن الحلم قريبا والطريق كان محفوفا بالتسهيلات لكني فعلتها**

**إلى من كلله الله بالهيبة والوقار الى من احمل اسمه بكل فخر إلى من لا ينفصل اسمه عن اسمي من كان مصدر الدعم والعطاء سندي وقوتي وملاذي بعد الله " أبي الغالي "**

**أهدي تخرجي وحصاد ما زرعته سنين طويلة في سبيل العلم الى اليد الخفيفة التي زالت عني طريق الأشواك وغرست فيا حب العلم والتعلم داعمي الاول والسند في رحلتي من أخذت بيدي لإكمال هذا الطريق " أمي الغالية "**

**إلى من وهبني الله نعمة وجودهم في حياتي الى العقد المتين**

**" أخواتي وأخي "**

**و إلى كل أصدقائي بدون استثناء إلى كل الأساتذة الأفاضل الذين قدموا لنا يد المساعدة إلى كل هؤلاء أهدي هذا العمل وفقني الله وإياكم إلى الخير**

**حميد اوجانة أحمد**

**الشكر و العرفان**

**الحمد لله الذي بنعمته تتم الصالحات، وبفضله وكرمه ينال الساعي ثمرة جهده.**

**أتقدم بأسمى عبارات الشكر والعرفان إلى أستاذتي الفاضلة، الدكتورة عجيلة حنان**

**مشرفة هذا العمل، لما أولاها لي من رعاية علمية وتوجيهات سديدة ونصائح غالية، كانت**

**نبراسًا أضاء لي درب البحث وأرشدني إلى سواء السبيل.**

**وأخيرا اشكر السادة الاساتذة أعضاء لجنة المناقشة على قبولهم وتكرمهم بمناقشة عملنا المتواضع.**

**الملخص :**

هدفت هذه الدراسة إلى تسليط الضوء على واقع أمن نظم المعلومات في مؤسسة خدمية جزائرية، حيث تناولت الإجراءات التقنية و الإدارية المعتمدة لأمن نظم المعلومات و المخاطر والتهديدات التي تواجه هذه النظم،. تم التركيز على حالة مؤسسة بريد الجزائر كنموذج تطبيقي يعكس التحديات الميدانية التي تواجهها المؤسسات في هذا المجال، وقد تم استخدام المنهج الوصفي لكونه يتناسب مع موضوع الدراسة، بالإضافة إلى الإعتماد على أسلوب دراسة حالة في جمع البيانات بواسطة استبيان تم تصميمه لتحقيق أغراض الدراسة،وقد تكونت عينة الدراسة من مجموعة الموظفين بمديرية برايد الجزائر بغرداية الذين لهم علاقة بموضوع الدراسة وبلغت عينة الدراسة (30) مفردة، وتم تحليل البيانات المحصلة باستخدام البرنامج الإحصائي (SPSS) ، وقد توصلت الدراسة إلى عدة نتائج، من أهمها: وجود قصور في الوعي الأمني لدى الموظفين، وضعف في تطبيق السياسات الأمنية، بالإضافة إلى الاعتماد على الحلول التقنية دون دعمها بالتدريب المستمر.

**الكلمات المفتاحية :** نظم المعلومات ، امن نظم المعلومات ، بريد الجزائر ،مؤسسات الخدمية

**Abstract:**

This study aimed to highlight the state of information systems security in an Algerian public service institution. It addressed the various risks and threats facing these systems, as well as the technical and administrative procedures adopted to protect them. The case of Algérie Poste was selected as an applied model that reflects the practical challenges faced by such institutions. A descriptive methodology was adopted, along with a case study approach, using a structured questionnaire developed to achieve the study’s objectives. The sample consisted of 30 employees from the Algérie Poste Directorate in Ghardaïa, who are directly involved in the subject. The collected data were analyzed using SPSS software, and the study concluded with several key findings, most notably: a lack of security awareness among employees, weak application of security policies, and an overreliance on technical solutions without sufficient training and continuous awareness efforts.

**Key words:** Information Security, Information Systems, , Algérie Poste, Public Service Institutions

**قائمة المحتويات**

|  |  |
| --- | --- |
| **الصفحة** | **العنوان** |
| **I** | **الاهداء** |
| **II** | **شكر و عرفان** |
| **III** | **الملخص** |
| **IV** | **قائمة المحتويات** |
| **VI** | **فهرس الاشكال** |
| **أ-ج** | **المقدمة** |
| **الفصل الأول الاطار النظري لامن نظم المعلومات في المؤسسات الخدمية** | |
| **01** | تمهيد |
| **26** | **المبحث الأول:** **الاطار النظري لامن نظم المعلومات في المؤسسات الخدمية** |
| **32** | **المبحت التاني : الدراسات السابقة** |
|  | **الفصل الثاني دراسة ميدانية** |
| **36** | تمهيد |
| **43** | **المبحث الأول :** تقديم عام للمؤسسة محل الدراسة و منهجية وأدوات الدراسة |
| **65** | **المبحث الثاني :** تحليل النتائج وإختبار الفرضيات |
| **66** | خلاصة |
| **69** | الخاتمة |
| **71** | قائمة المصادر و المراجع |
| **80** | الملاحق |
| **83** | فهرس |

**قائمة الجداول والأشكال والملاحق**

|  |  |  |
| --- | --- | --- |
| ص | العبارة | الشكل |
| 31 | يمثل المقارنة بين الدراسات السابقة والدراسة الحالية | 1-1 |
| 40 | الإحصائية الخاصة باستمارة الاستبيان | 01-2 |
| 41 | عدد فقرات كل بعد | 02-2 |
| 42 | نتائج تحليل الثبات | 03-2 |
| 43 | نتائج اختبار التوزيع الطبيعي | 04-2 |
| 44 | يمثل أعمار أفراد العينة | 05-2 |
| 45 | مثل تقسيم المستوى التعليمي لأفراد العينة | 06-2 |
| 46 | يمثل تقسيم وظائف أفراد العينة | 07-2 |
| 46 | يمثل تقسيم سنوات الخبرة لأفراد العينة | 08-2 |
| 41 | يمثل التكرارت والنسب المئوية للبعد الأول | 09-2 |
| 49 | يمثل التكرارت والنسب المئوية للبعد الثاني | 10-2 |
| 53 | يمثل التكرار والنسب المئوية للبعد الثالث | 11-2 |
| 58 | يمثل تفسير النتائج للبعد الأول | 12-2 |
| 60 | يمثل تفسير النتائج للبعد الثاني | 13-2 |
| 61 | يمثل تفسير النتائج للبعد الثالث | 14-2 |

**قائمة الجداول**

**قائمة الاشكال**

|  |  |  |
| --- | --- | --- |
| ص | العبارة | الرقم |
| 92 | الاستبيان | 01-2 |
| 95 | مخرجات spss | 02-2 |
| 97 | قائمة الاساتدة المحكمين | 03-2 |
| 99 | الفهرس | 04-2 |

|  |  |  |
| --- | --- | --- |
| **رقم الشكل** | **عنوان الشكل** | **الصفحة** |
| **شكل (2-1)** | يوضح الهيكل التنظيمي لمديرية الجزائر وحدة غرداية | **46** |

**قائمة الملاحق**

**مقدمة**

**توطئة**:

في ظل التحول الرقمي المتسارع الذي يشهده العالم اليوم، أصبحت المعلومات تُعد من بين أهم الأصول الاستراتيجية التي تعتمد عليها المؤسسات في تحقيق أهدافها وتنفيذ مهامها. ولم تعد المعلومات مجرد بيانات يتم تداولها أو تخزينها، بل تحولت إلى عنصر محوري في دعم اتخاذ القرار، وتحسين الأداء المؤسسي، وتعزيز القدرة التنافسية. وتبرز هذه الأهمية بشكل خاص في المؤسسات الخدمية، التي تعتمد بدرجة كبيرة على نظم المعلومات الإلكترونية في تقديم خدماتها للمواطنين والعملاء، وضمان جودة الخدمة، وسرعة الاستجابة، وكفاءة العمليات، وتتجلى هذه النظم في مختلف المجالات، من نظم إدارة علاقات العملاء، إلى قواعد البيانات المركزية، وأنظمة الحجز، ونظم الموارد البشرية والمالية، وغيرها من المنصات التي تمثل البنية التحتية الرقمية للمؤسسة. ومع هذا الاعتماد المتزايد على تكنولوجيا المعلومات، برزت الحاجة الماسّة إلى ضمان أمن هذه النظم وحماية البيانات التي تحتويها من مختلف التهديدات والمخاطر، ويُعد أمن المعلومات اليوم أحد أبرز التحديات التي تواجه المؤسسات في العصر الرقمي، حيث تواجه هذه المؤسسات مجموعة متنوعة من التهديدات، سواء كانت داخلية (مثل الأخطاء البشرية ضعف الوعي الأمني الفساد الإداري) أو خارجية (مثل الهجمات السيبرانية، الفيروسات، الإختراقات). وقد يؤدي أي اختراق أمني إلى عواقب وخيمة تطال جوانب متعددة، مثل سمعة المؤسسة، وثقة العملاء، والامتثال للمتطلبات القانونية والتنظيمية، فضلاً عن الخسائر المادية والتوقف عن تقديم الخدمات.

**إشكالية الدراسة:**

رغم التطور الحاصل في تقنيات الحماية، لا تزال المؤسسات الخدمية في الجزائر – مثل بريد الجزائر – تواجه صعوبات حقيقية في تأمين بياناتها وضمان استمرارية خدماتها. ومن هنا تطرح الإشكالية التالية نفسها:

ما واقع تطبيق آمن نظم المعلومات في مؤسسة بريد الجزائر وحدة غرداية ؟ وماهي أهم المعوقات التي تواجهها في هدا الجانب؟

**الأسئلة الفرعية:**

1. هل تساهم البيئة الإدارية في تفعيل آمن نظم المعلومات في مؤسسة بريد الجزائر وحدة غرداية؟

2. ما هي أهم أساليب امن نظم المعلومات التي تستخدمها مؤسسة بريد الجزائر وحدة غرداية؟

3. ماهي أهم المعوقات التي تواجهها مؤسسة بريد الجزائر وحدة غرداية عند تطبيق امن نظم

المعلومات ؟

**الفرضيات**

**الفرضية الرئيسية:**

تقوم مؤسسة بريد الجزائر وحدة غرداية بتطبيق أمن نظم المعلومات في تسيير خدماتها

**الفرضية الفرعية الاولى  :**

تساهم البيئة الإدارية في تفعيل أمن نظم المعلومات في مؤسسة بريد الجزائر وحدة غرداية.

**الفرضية الفرعية الثانية :**

تستخدم مؤسسة بريد الجزائر وحدة غرداية عدة أساليب لأمن نظم المعلومات.

**الفرضية الفرعية الثالثة :**

تواجه مؤسسة بريد الجزائر وحدة غرداية عدة معوقات عند تطبيق امن نظم المعلومات.

**أهمية الدراسة:**

تسليط الضوء على أحد التحديات الحيوية التي تواجه المؤسسات الخدمية في ظل التحول الرقمي، والمتمثل في أمن وحماية المعلومات.  
المساهمة في توعية المؤسسات الجزائرية، خصوصًا الخدمية منها، بأهمية تطبيق إجراءات فعالة لأمن المعلومات.  
تقديم أداة لتقييم واقع أمن المعلومات داخل المؤسسات، مما يساعد في الكشف عن نقاط الضعف والثغرات.  
دعم جهود تحسين الأداء المؤسسي من خلال تعزيز الحماية المعلوماتية وتقليل المخاطر الإلكترونية.  
تعزيز ثقة المتعاملين مع هذه المؤسسات عبر ضمان سرية المعلومات وسلامتها وتوفرها.

**أهداف الدراسة:**

التعرف على المفاهيم الأساسية ومكونات نظم أمن المعلومات؛

تحليل التحديات والتهديدات التي تواجه المؤسسات الخدمية في هذا المجال؛

إبراز الأساليب والإجراءات التقنية والإدارية المعتمدة لتحقيق الأمن المعلوماتي؛

تقديم مقترحات عملية لتحسين نظم أمن المعلومات في المؤسسات الخدمية الجزائرية.

**المنهج المتبع:**

تم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي، من خلال الجمع بين الدراسة النظرية لمفاهيم أمن المعلومات، والتحليل الميداني لواقع تطبيقها داخل مؤسسة بريد الجزائر كنموذج للمؤسسات الخدمية.

**حدود الدراسة :**

1. الحدود المكانية : تم إسقاط الجانب النظري لهذه الدراسة على واقع مؤسسة عمومية من خلال دراسة حالة مديرية بريد الجزائر وحدة غرداية؛

2الحدود الزمنية : تم إنجاز هذه الدراسة في الفترة الممتدة من 20 مارس الى 21 ماي 2025

3 الحدود البشرية : إقتصرت الدراسة على عينة مكونة من الموظفين في مديرية بريد الجزائر وحدة غرداية.

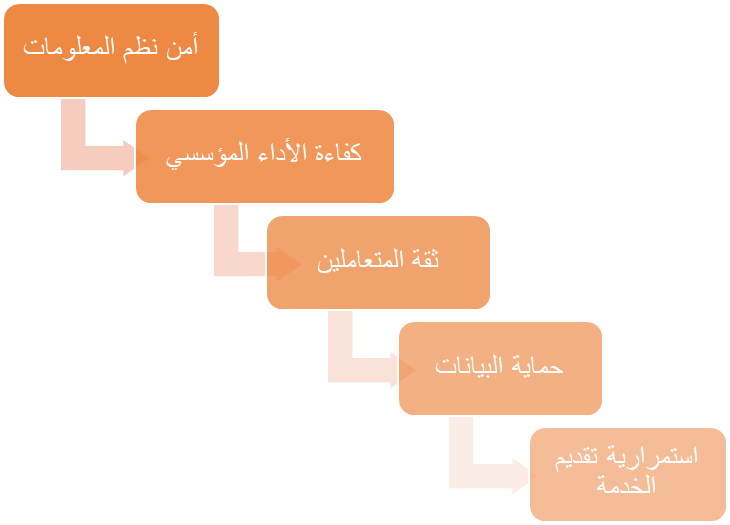
**هيكل الدراسة :**

بهدف الإجابة على الإشكالية المطروحة قسمنا بحثنا إلى فصلين وهما كالاتي :

**الفصل الاول:** دراسة عن الاطار النظري حول أمن المعلومات في المؤسسات الخدمية وقد اشتمل مبحثين حيث المبحث الأول قسم الى ثلاث مطالب فقد تطرق المطلب الاول الى مدخل عام حول أمن نظم المعلومات اما المطلب الثاني حول التهديدات والتحديات التي تواجه أمن المعلومات وأما المطلب الثالث فكان حول سبل حماية أمن المعلومات في المؤسسات الخدمية, ثم تطرقنا الى المبحث الثاني وكان حول الدراسات السابقة وقد قسمناه الى ثلاث مطالب,المطلب الاول كان حول الدراسات العربية والمطلب الثاني حول الدراسات الأجنبية اما المطلب الثالث فكان مقارنة بين الدراسة الحالية والدراسات السابقة.

**الفصل الثاني:**  تطرقنا في الفصل الثاني الى دراسة حالة ,حيث قسم الى مبحثين, المبحث الأول كان تقديم عام للمؤسسة ومنهجية وأدوات الدراسة, وفد قسم الى مطالبين تضم تقديم المؤسسة وطرق وأدوات الدراسة , أما المبحث الثاني كان حول تحليل النتائج واختبار الفرضيات وقد قسم الى مطلبين وتناولنا فيه تحليل فقرات الدراسة وتفسير النتائج واختبار الفرضيات.

**نمودج الدراسة:**



**الفصل الأول:**

**الاطار النظري لامن نظم المعلومات في المؤسسات الخدمية**

### 

### **تمهيد**

يشكل أمن المعلومات في العصر الرقمي ركيزة أساسية لضمان استمرارية العمل وجودة الخدمات داخل المؤسسات، لاسيما المؤسسات الخدمية التي تعتمد بشكل كبير على المعلومات في أداء مهامها اليومية. ومع تزايد الاعتماد على النظم المعلوماتية، أصبحت هذه الأخيرة عرضة لمجموعة متزايدة من التهديدات والمخاطر الأمنية، سواء من داخل المؤسسة أو خارجها، مما يجعل من الضروري دراسة وفهم نظم أمن المعلومات من منظور شامل يراعي مختلف الجوانب التقنية، الإدارية، والتشريعية

يهدف هذا الفصل إلى بناء قاعدة معرفية قوية تشكل الإطار النظري للدراسة، من خلال تسليط الضوء على المفاهيم الأساسية المرتبطة بنظم أمن المعلومات، وأهميتها المتزايدة في بيئة المؤسسات الخدمية. كما يتناول الفصل أنواع هذه المؤسسات، ودور نظم الأمن في تحسين جودة خدماتها، إلى جانب التهديدات والتحديات الأمنية التي تواجهها، والأساليب التقنية والإدارية المعتمدة لضمان حماية المعلومات

سيتدرج الفصل في تناول هذه المحاور وفق تنظيم منهجي يبدأ بتوضيح المفاهيم الأساسية، ثم ينتقل إلى استعراض السياق المؤسسي، ومن ثم تحليل المخاطر الأمنية، فاستعراض أدوات وتقنيات الحماية، قبل أن يختتم باستعراض السياسات والإجراءات الإدارية التي تعزز أمن المعلومات داخل المؤسسات الخدمية.

### **المبحث الأول : الاطار النظري لأمن نظم المعلومات**

شهد العالم في العقود الأخيرة تطورًا متسارعًا في مجال تكنولوجيا المعلومات، حيث أصبحت النظم المعلوماتية عنصرًا محوريًا في عمل المؤسسات بمختلف أنواعها. ومع هذا الاعتماد المتزايد، برزت الحاجة الماسّة إلى حماية هذه النظم من المخاطر والتهديدات التي قد تؤثر على سريّة المعلومات وسلامتها وتوافرها، مما أدى إلى بروز مفهوم نظم أمن المعلومات كأحد الركائز الأساسية لضمان استقرار العمل المؤسسي والحفاظ على البيانات.

يهدف هذا المبحث إلى تقديم مدخل مفاهيمي شامل حول نظم أمن المعلومات، من خلال التطرق إلى نشأتها وتعريفها، وأهدافها، ثم الانتقال إلى تحديد أبرز مكوناتها، والمتمثلة في مبادئ السرية، السلامة، والتوافر. كما سيتم تسليط الضوء على الأهمية المتزايدة لهذه النظم في بيئة المؤسسات الخدمية، بالنظر إلى طبيعة المعلومات الحساسة التي تتعامل معها.

### **المطلب الأول : مدخل عام حول أمن نظم المعلومات**

#### **الفرع الأول:** **مفهوم نظم أمن المعلومات (تعريف، نشأة)**

#### **أولا: تعريف أمن المعلومات**

* **التعريف الأول**

هو مجموع الإجراءات والتدابير المستخدمة في المحالين الإداري والفني الحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة الإجراءات خاطئة أو غير الوافية

المستخدمة من إدارة هذه المصادر.[[1]](#footnote-1)

### **التعريف الثاني:**

هوحماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي

على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل ـ المعالجة).[[2]](#footnote-2)

* **التعريف الثالث**

عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة التداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضا لمخاطر الاختراق .[[3]](#footnote-3)

جميع هذه التعريفات تشترك في فكرة أن نظم أمن المعلومات هي مجموعة من السياسات والتكنولوجيا والإجراءات المصممة لحماية المعلومات من التهديدات المختلفة، مع التركيز على تحقيق السرية والسلامة والتوافر. ومع ذلك، تختلف المصادر في التركيز على الجوانب الفنية أو الإدارية أو الاستراتيجية لهذه النظم.

نظم أمن المعلومات هي مجموعة من السياسات والإجراءات والتكنولوجيا المصممة لحماية المعلومات من الوصول غير المصرح به أو التعديل أو التدمير، بهدف تحقيق السرية والسلامة والتوافر، مع اختلاف طفيف في التفاصيل بين المصادر المختلفة.

### **ثانيا: نشأة نظم أمن المعلومات**

بدأت نظم أمن المعلومات تأخذ شكلها الحالي في ظل الحاجة المتزايدة لحماية البيانات الرقمية التي أصبحت أساس عمل المؤسسات في العالم المعاصر. في البداية، كان مفهوم "أمن المعلومات" يقتصر بشكل رئيسي على حماية الأجهزة والبيانات من الهجمات الخارجية، لكن مع تطور الإنترنت والتكنولوجيا الرقمية، أصبحت المؤسسات بحاجة إلى استراتيجيات أكثر تطورًا لضمان سلامة المعلومات وحمايتها من التهديدات المتنوعة.[[4]](#footnote-4)

كانت أولى محاولات تأمين المعلومات تعود إلى العقود الأولى من القرن العشرين، حيث كانت المؤسسات تعتمد على تدابير بسيطة مثل كلمات المرور وحماية الأجهزة من الفيروسات. ومع انتشار أجهزة الكمبيوتر في المؤسسات في السبعينات والثمانينات، بدأت تظهر تحديات جديدة مثل الهجمات السيبرانية التي تسببت في تسريب البيانات، مما استدعى تطوير أساليب وتقنيات حديثة أكثر تعقيدًا

بحلول التسعينات، شهدت نظم أمن المعلومات تحولًا جذريًا. فقد بدأ يشمل تأمين الشبكات، وحماية البيانات عبر الإنترنت، بالإضافة إلى حماية الأنظمة الداخلية من الهجمات السيبرانية مثل الفيروسات والبرمجيات الضارة. كان لهذه الحقبة دور في إدراك المؤسسات الحكومية والخدمية أهمية تكنولوجيا الحماية المتقدمة، والتي بدأت تشمل التشفير، جدران الحماية، أنظمة كشف التسلل، وأنظمة المراقبة المستمرة.[[5]](#footnote-5)

ومع بداية القرن الواحد والعشرين، زادت الهجمات الرقمية بشكل ملحوظ، وأصبحت المؤسسات تواجه تهديدات متنوعة مثل الهجمات المعقدة من القراصنة، والفيروسات الضارة التي يمكن أن تُسرب أو تدمر البيانات الحساسة. في هذا السياق، تطور مفهوم "أمن المعلومات" ليشمل سياسات شاملة لحماية جميع الجوانب المتعلقة بالبيانات والمعلومات، سواء كانت حساسة أو غير حساسة، وذلك باستخدام تقنيات مثل التشفير المتقدم، أدوات الكشف عن التسلل، والسياسات التي تضمن وجود دفاعات متعددة المستويات

ومع التحديات المتزايدة، بدأ التركيز على حوكمة أمن المعلومات بشكل كبير، حيث تم تطوير معايير وأطر عمل مثل **ISO 27001** الخاصة بنظم إدارة أمن المعلومات، بالإضافة إلى القوانين والتشريعات التي تعزز حماية المعلومات، مثل **قانون حماية البيانات العامة** في الاتحاد الأوروبي أصبحت الحوكمة جزءًا أساسيًا من استراتيجية أمن المعلومات داخل المؤسسات الخدمية ، التي تطلبت تحصينًا شاملاً للأنظمة والمعلومات لضمان تقديم خدمات آمنة للمواطنين.[[6]](#footnote-6)

ومع استمرار تقدم التكنولوجيا، يواجه أمن المعلومات تحديات جديدة مثل الهجمات الرقمية المعقدة التي قد تستهدف أنظمة الذكاء الاصطناعي، البلوك تشين، وتقنيات الحوسبة السحابية. ومع تزايد استخدام هذه التقنيات في المؤسسات الخدمية، أصبح من الضروري تكامل أساليب جديدة للحماية تشمل الذكاء .الاصطناعي والتعلم الآلي لتعزيز قدرة الأنظمة على مواجهة التهديدات

**الفرع التاني : مكونات نظم أمن المعلومات (السرية، السلامة، التوافر)**

تعتبر مكونات نظم أمن المعلومات الأساسية هي الأسس التي تقوم عليها جميع استراتيجيات الحماية في المؤسسات، وهي: **السرية**، **السلامة**، و**التوافر**. هذه المبادئ تعتبر حجر الزاوية في ضمان حماية المعلومات في ظل التهديدات المتزايدة التي تواجهها المؤسسات في العصر الرقمي. تتكامل هذه المكونات لتوفير بيئة آمنة ومحمية للبيانات والمعلومات، حيث كل مكون يركز على جانب محدد من حماية البيانات والمعلومات ويكمل الجوانب الأخرى لضمان استمرارية الأمان في النظام المعلوماتي.

#### **السرية :**

تعني السرية حماية المعلومات من الوصول غير المصرح به، سواء من خلال الاطلاع عليها أو كشفها أو استخدامها بطرق قد تضر بصاحبها بشكل مباشر أو غير مباشر. ومن هذا المنطلق، من الضروري تحديد طبيعة استخدام المعلومات التي نمتلكها، وما إذا كانت تتطلب مستوى معينًا من الخصوصية، بالإضافة إلى منح صلاحيات محددة لأطراف معينة، كالسماح بالقراءة أو التعديل أو التحكم الكامل

بها.[[7]](#footnote-7)

#### **السلامة :**

ضرورة التأكد من بقاء المعلومات على حالها دون تعديل أو حذف من جهات غير معروفة أو غير مخولة.أما من ناحية الإتاحة، فرغم أهمية الحفاظ على سرية المعلومات وسلامتها، إلا أن قيمتها تقل إذا تعذر الوصول إليها أو استغرق ذلك وقتًا طويلاً."[[8]](#footnote-8)

تتم حماية السلامة من خلال :

**التقنيات الرقمية مثل التحقق من السلامة** : تضمن أن البيانات لم يتم تعديلها

**التحقق المزدوج والتدقيق**: استخدام آليات تدقيق وتحقق من صحة البيانات بشكل مستمر

**النسخ الاحتياطي المنتظم**: لتجنب فقدان البيانات بسبب الحوادث أو التلاعب

#### **التوافر :**

ضمان استمرارية عمل تكنولوجيا المعلومات، والقدرة المتواصلة على التفاعل مع البيانات وتقديم الخدمات المعلوماتية في الوقت المناسب، مع حماية مستخدمي المعلومات من أي أضرار قد تنتج عن استخدامها أو الوصول إليها.[[9]](#footnote-9)

### **العلاقة بين المكونات الثلاثة**

تعتبر مكونات **السرية**، **السلامة**، و**التوافر** مترابطة بشكل وثيق، حيث أن كل مكون يلعب دورًا مكملًا للآخر. على سبيل المثال، في حالة عدم توفر البيانات (التوافر) أو في حال حدوث خلل في مصداقية البيانات (السلامة)، فإن السرية قد تصبح عرضة للخطر. بالتالي، لا يمكن لأي مكون من هذه المكونات أن يعمل بشكل فعال بدون المكونات الأخرى. ولذا، يجب على المؤسسات ضمان تكامل هذه المكونات في إطار شامل من السياسات والإجراءات الأمنية.

### **الفرع الثالث : أهمية أمن المعلومات في المؤسسات الخدمية**

في العصر الرقمي الذي نعيشه، أصبحت البيانات والمعلومات هي الأصل الأكثر قيمة للمؤسسات بمختلف أنواعها، وخاصة المؤسسات الخدمية التي تعتمد بشكل كبير على تبادل المعلومات مع العملاء والشركاء. ومع التطور التقني المتسارع، ظهرت تحديات جديدة تتعلق بحماية هذه المعلومات من التهديدات السيبرانية والاختراقات الأمنية. لذلك، أصبح أمن المعلومات ضرورة استراتيجية لضمان استمرارية الأعمال وتعزيز الثقة بين المؤسسات والعملاء.

في هذا السياق، سيتم تسليط الضوء على أهمية أمن المعلومات في المؤسسات الخدمية من خلال عدة محاور رئيسية، بما يشمل الحماية القانونية، والحفاظ على الثقة، ودعم العمليات التشغيلية، وتقليل التكاليف الناتجة عن الحوادث الأمنية.[[10]](#footnote-10)

### **1-حماية البيانات الحساسة للعملاء :**

المؤسسات الخدمية مثل البنوك، شركات الاتصالات، والمستشفيات تعتمد بشكل كبير على جمع ومعالجة بيانات العملاء الشخصية (مثل أرقام الهوية، عناوين الإقامة، وأرقام الحسابات البنكية).

**أهمية الحماية:**

أي خرق لهذه البيانات يمكن أن يؤدي إلى فقدان الثقة، وزيادة المخاطر القانونية، وحتى تعرض العملاء للضرر المباشر (مثل سرقة الهوية أو الاحتيال المالي.(

وفقًا لتقرير شركة IBM (2022)، فإن متوسط تكلفة خرق البيانات في المؤسسات الخدمية بلغ حوالي **4.4 مليون دولار**، مما يعكس أهمية الاستثمار في أمن المعلومات.

### **2-تحقيق الامتثال للقوانين واللوائح :**

مع تنامي الوعي بأهمية حماية البيانات، تم إصدار العديد من القوانين الدولية والمحلية التي تفرض على المؤسسات الخدمية اتخاذ إجراءات صارمة لتأمين المعلومات.

**أمثلة على القوانين:**

اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي

قانون حماية البيانات الشخصية (PDPL) في المملكة العربية السعودية

قانون الصحة الإلكترونية (HIPAA) في الولايات المتحدة

### **3-تعزيز الثقة بين المؤسسات والعملاء:**

ثقة العملاء هي أحد الركائز الأساسية لنجاح أي مؤسسة خدمية

**4-دور أمن المعلومات:**

عندما يشعر العملاء بأن بياناتهم محمية بشكل جيد، فإنهم يصبحون أكثر ولاءً للمؤسسة

على سبيل المثال، البنوك التي تستثمر في أمن المعلومات تتمتع بسمعة قوية، مما يعزز ثقة العملاء في استخدام خدماتها الرقمية مثل التحويلات المالية عبر الإنترنت.[[11]](#footnote-11)

### **5-ضمان استمرارية الأعمال :**

المؤسسات الخدمية تعتمد بشكل كبير على الأنظمة الرقمية في تقديم خدماتها[[12]](#footnote-12)

**أهمية الاستمرارية:**

أي انقطاع في الخدمات نتيجة لهجوم إلكتروني يمكن أن يؤدي إلى خسائر مالية كبيرة وتأثير سلبي على سمعة المؤسسة.

على سبيل المثال، الهجمات على أنظمة المستشفيات قد تؤدي إلى تعطل الوصول إلى السجلات الطبية، مما يهدد حياة المرضى.

**دراسة حالة:**

في عام 2021، تعرضت شركة Colonial Pipeline الأمريكية لهجوم إلكتروني، مما أدى إلى تعطيل توزيع الوقود في عدة ولايات لمدة أسبوع، وأثر بشكل مباشر على الاقتصاد الأمريكي.

### **6-تقليل التكاليف الناتجة عن الحوادث الأمنية :**

الحوادث الأمنية مثل اختراق البيانات أو هجمات الفدية يمكن أن تكون مكلفة للغاية.

**أهمية التقليل:**

الاستثمار في أمن المعلومات يمكن أن يقلل من احتمالية حدوث هذه الحوادث، وبالتالي تقليل التكاليف المرتبطة بها .

وفقًا لدراسة أجراها المعهد القومي للمعايير والتكنولوجيا (NIST)، فإن المؤسسات التي تعتمد على استراتيجيات أمنية متقدمة تحقق وفورات تصل إلى **60%** في تكلفة التعامل مع الحوادث.

### **7-دعم التحول الرقم:**

مع تزايد اعتماد المؤسسات الخدمية على التحول الرقمي، أصبح أمن المعلومات جزءًا لا يتجزأ من هذه العملية.

**أهمية الدعم** :

بدون أمن معلومات قوي، لن تتمكن المؤسسات من الاستفادة الكاملة من الحلول الرقمية مثل الذكاء الاصطناعي، إنترنت الأشياء، والخدمات السحابية .

على سبيل المثال، الشركات التي تقدم خدمات التعليم عبر الإنترنت تحتاج إلى ضمان أمان المنصات التعليمية لحماية بيانات الطلاب والمعلمين.

### **8-تحسين الكفاءة التشغيلية :**

أنظمة أمن المعلومات ليست فقط للحماية، بل يمكن أن تساهم في تحسين الكفاءة التشغيلية.

**أهمية الكفاءة:**

من خلال استخدام أدوات مثل تحليل البيانات وإدارة الوصول، يمكن للمؤسسات تبسيط العمليات وتقليل الأخطاء البشرية.

على سبيل المثال، أنظمة إدارة الهوية والوصول تساعد في تحسين إدارة الموظفين والعملاء.

### **9-مواجهة التهديدات المتزايدة :**

مع زيادة التهديدات السيبرانية، أصبحت المؤسسات الخدمية مستهدفة بشكل مباشر.

**أهمية المواجهة:**

الهجمات السيبرانية مثل هجمات الحرمان من الخدمة وهجمات الفدية أصبحت أكثر تعقيدًا وانتشارًا

المؤسسات التي تستثمر في الدفاع السيبراني تكون أكثر قدرة على مواجهة هذه التهديدات.

### **10-تعزيز التعاون الآمن**

### المؤسسات الخدمية غالبًا ما تعمل مع شركاء وموردين مختلفين، مما يتطلب تبادل البيانات بشكل آمن.

**أهمية التعاون**

أمن المعلومات يضمن أن البيانات المشتركة محمية أثناء النقل والتخزين .

على سبيل المثال، شركات التأمين التي تتعاون مع المستشفيات تحتاج إلى ضمان أمان بيانات المرضى.

**المطلب الثاني : التهديدات والتحديات التي تواجه أمن المعلومات**

تواجه المؤسسات الخدمية، ، مجموعة من التحديات الأمنية التي تتنوع ما بين تهديدات داخلية تنجم عن العامل البشري أو ضعف الإجراءات الأمنية، وتهديدات خارجية مثل الهجمات السيبرانية، والبرمجيات الخبيثة، والتجسس الإلكتروني. إضافة إلى ذلك، تزداد المخاطر نتيجة القصور في الإطار القانوني والتشريعي المنظم لأمن المعلومات، مما يخلق بيئة معقدة تتطلب جهودًا متكاملة بين العنصر البشري والتقني والإداري للتعامل مع هذه المخاطر بكفاءة وفعالية.

يهدف هذا المبحث إلى تحليل هذه التهديدات من خلال تقسيمها إلى فئات رئيسية: **التهديدات الداخلية**، و**التهديدات الخارجية**، و**التحديات القانونية والتشريعية**، مع تقديم أمثلة واقعية لتوضيح أثرها على أمن المعلومات في المؤسسات الخدمية، واستعراض السبل الممكنة للحد من آثارها وتجنبها.

### **الفرع الأول : التهديدات الداخلية (الأخطاء البشرية، ضعف الوعي الأمني، الفساد الإداري(**

في بيئة العمل الحديثة، لم تعد التهديدات التي تواجه أمن المعلومات تقتصر على الهجمات الخارجية فحسب، بل أصبحت التهديدات الداخلية تمثل تحدياً حقيقياً ومتصاعداً، خصوصاً في المؤسسات الخدمية التي تتعامل يومياً مع كمّ هائل من البيانات الحساسة المرتبطة بالموظفين والعملاء والأنظمة التشغيلية. وتبرز هذه التهديدات عادة من داخل المؤسسة نفسها، من قبل موظفين أو إداريين، سواء عن قصد أو عن غير قصد، مما يجعل اكتشافها والتحكم فيها أكثر صعوبة مقارنة بالتهديدات الخارجية.

#### **أولا: الأخطاء البشرية**

تُعد الأخطاء البشرية من أكثر أسباب الانتهاكات الأمنية شيوعاً في المؤسسات الخدمية. فعلى الرغم من تطوير الأنظمة الأمنية المعقدة، إلا أن الإنسان يظل الحلقة الأضعف في منظومة الأمن السيبراني. ومن أبرز هذه الأخطاء: النقر على روابط ضارة في رسائل البريد الإلكتروني، حذف أو تعديل ملفات مهمة عن غير قصد، استخدام كلمات مرور ضعيفة أو إعادة استخدامها، أو حتى ترك أجهزة الحاسوب مفتوحة دون مراقبة. وقد بينت الدراسات أن أكثر من 60% من الحوادث الأمنية في بعض المؤسسات تعود في الأساس إلى تصرفات بشرية غير مدروسة.

إن سبب انتشار هذه الأخطاء يعود غالباً إلى غياب التكوين الكافي أو عدم إدراك الموظف لحساسية البيانات التي يتعامل معها يومياً، مما يفتح المجال أمام العديد من الثغرات التي قد تستغلها الجهات الخارجية.[[13]](#footnote-13)

#### **ثانيا: ضعف الوعي الأمني**

يرتبط هذا الجانب بشكل مباشر بالأخطاء البشرية، ويُعد أحد أبرز مسببات الاختراقات المعلوماتية الداخلية. فالكثير من العاملين في المؤسسات الخدمية لا يملكون ثقافة أمنية رقمية كافية تؤهلهم للتصرف الصحيح في حال وقوع تهديد محتمل. فهم، في الغالب، يجهلون مفاهيم أساسية مثل الهندسة الاجتماعية، وتقنيات التصيد الإلكتروني ، أو كيفية التحقق من موثوقية الروابط والمرفقات.[[14]](#footnote-14)

تتجلى مظاهر ضعف الوعي الأمني في استخدام الشبكات العامة غير المؤمنة أثناء العمل، أو مشاركة كلمات المرور مع الزملاء، أو تدوين معلومات حساسة في أماكن يسهل الوصول إليها. كل ذلك يجعل المؤسسة عرضة لتهديدات داخلية قد تؤدي إلى تسريب بيانات العملاء أو توقف الأنظمة عن العمل.

#### **ثالثا: الفساد الإداري**

على خلاف الأخطاء البشرية وضعف الوعي، فإن الفساد الإداري يُعد تهديداً داخلياً متعمداً، ويأخذ أشكالاً متعددة مثل: تسريب معلومات سرية إلى جهات خارجية، بيع بيانات المستخدمين، تعطيل الأنظمة بهدف تمرير صفقات غير قانونية، أو حتى التغاضي المتعمد عن ثغرات أمنية لأهداف شخصية. ويُعتبر هذا النوع من التهديدات الأخطر لأنه ينبع من أشخاص لديهم صلاحيات أو اطلاع على معلومات حساسة، ما يجعل الكشف عنه أكثر تعقيدا.

وتزداد خطورة هذا النوع من التهديدات في المؤسسات الخدمية الكبرى، مثل المؤسسات البريدية أو المصرفية، حيث يمكن أن يؤدي هذا الفساد إلى الإضرار بثقة العملاء وتعرض المؤسسة لمساءلة قانونية لمواجهة هذه التهديدات، لا بد من وضع سياسة أمن معلومات متكاملة تعتمد على ثلاثة محاور رئيسية: **الوقاية** من خلال التكوين والتدريب المستمر، **الرقابة** عبر أنظمة مراقبة وسجلات استخدام دقيقة، و**الردع** من خلال قوانين صارمة تُطبق على كل من يثبت تورطه في أي فعل يمس بأمن المعلومات.

### **الفرع التاني : : التهديدات الخارجية (الهجمات السيبرانية، الفيروسات، الاختراقات(**

تمثل التهديدات الخارجية أحد أخطر التحديات التي تواجه أمن المعلومات، خصوصاً في المؤسسات الخدمية التي تعتمد بشكل أساسي على نظم إلكترونية لمعالجة وتخزين البيانات، مثل البريد، البنوك، المستشفيات، والجامعات. وتنبع خطورة هذه التهديدات من كونها صادرة عن أطراف خارجية غالباً ما تكون مجهولة، تستخدم تقنيات متقدمة وأساليب اختراق معقدة يصعب أحيانًا رصدها أو التنبؤ بها.

في عالم مترابط يعتمد على الإنترنت، لم تعد الجدران التقليدية للمؤسسات كافية لحمايتها. بل أصبح من الضروري التفكير في الأمن من منظور شامل، يشمل التحصين التقني، والتدريب البشري، والتشريعات القانونية. وتتنوع التهديدات الخارجية التي تواجه المؤسسات الخدمية، ومن أبرزها: **الهجمات السيبرانية**، **الفيروسات**، و**الاختراقات.[[15]](#footnote-15)**

#### **أولاً: الهجمات السيبرانية**

الهجمات السيبرانية هي محاولات متعمدة لتعطيل أو تدمير أنظمة المعلومات، أو الوصول غير المصرح به إلى بيانات سرية. وتأتي هذه الهجمات في أشكال متعددة، مثل هجمات حجب الخدمة (DDoS)، والهجمات باستخدام برمجيات الفدية (Ransomware)، وهجمات التصيد (Phishing) والهندسة الاجتماعية.

في المؤسسات الخدمية، يمكن أن تؤدي هذه الهجمات إلى شلل تام في تقديم الخدمات، أو تسريب معلومات حساسة خاصة بالمستخدمين. فعلى سبيل المثال، يمكن أن تتعرض منصة بريد إلكتروني تابعة لمؤسسة خدمية لهجوم DDoS يتسبب في تعطيل التواصل مع المواطنين لعدة ساعات أو أيام، ما يؤثر على سمعة المؤسسة وثقة العملاء.

#### **ثانياً: الفيروسات والبرمجيات الخبيثة**

تُعد الفيروسات من أقدم أشكال التهديدات الخارجية، لكنها ما تزال تحتفظ بخطورتها، خاصة مع تطورها إلى برمجيات أكثر تعقيداً مثل "Trojan Horses"، و"Worms"، و"Spyware"، و"Rootkits". تعمل هذه البرمجيات على التسلل إلى الأنظمة، وتخريب البيانات، أو التجسس على المستخدمين دون علمهم

في السياق الخدمي، يمكن لفيروس بسيط أن يتسبب في ضياع بيانات عملاء، أو تلف ملفات مالية مهمة، أو حتى التحكم في أنظمة الإدارة عن بُعد. وتكمن خطورة الفيروسات في قدرتها على الانتقال بسرعة من جهاز إلى آخر داخل الشبكة، ما يجعل عملية احتوائها معقدة ومكلفة.

#### **ثالثاً: الاختراقات**

الاختراق هو عملية دخول غير مشروع إلى أنظمة المعلومات، ويهدف عادة إلى سرقة البيانات أو تعديلها أو حذفها. ويقوم بها أفراد أو جماعات يعرفون بالـ"هاكرز"، وقد يكون الدافع وراءهم سياسيًا، ماليًا، أو حتى مجرد التحدي التقني.

تتعرض المؤسسات الخدمية لمحاولات اختراق مستمرة، خاصة تلك التي تحتوي على بيانات المواطنين أو المعلومات المالية أو السجلات الطبية. في حالة نجاح عملية الاختراق، يمكن أن تتعرض المؤسسة لخسائر فادحة سواء من حيث السمعة أو من الناحية المادية، بالإضافة إلى إمكانية تعرضها لمتابعات قانونية إذا ثبت فشلها في حماية بيانات المستخدمين.[[16]](#footnote-16)

### **سبل الحماية:**

* لمواجهة هذه التهديدات، يجب على المؤسسات الخدمية تبني مجموعة من الإجراءات الوقائية، مثل:
* تحديث أنظمة التشغيل والبرمجيات باستمرار
* استخدام برامج الحماية المتقدمة وجدران الحماية
* مراقبة الشبكات بشكل دائم واكتشاف السلوكيات المشبوهة
* تدريب الموظفين على كيفية التعامل مع الرسائل المجهولة أو المشبوهة
* الاعتماد على أنظمة النسخ الاحتياطي والاسترداد السريع

### **الفرع الثالث : : التحديات القانونية والتشريعية المتعلقة بحماية المعلومات**

في ظل الثورة الرقمية والتطور الهائل في تكنولوجيا المعلومات، أصبحت حماية المعلومات من القضايا الجوهرية التي تشغل اهتمام الحكومات والمؤسسات في مختلف أنحاء العالم، وخاصة المؤسسات الخدمية التي تتعامل مع بيانات حساسة تخص الأفراد والمجتمع. وتفرض هذه البيئة الجديدة تحديات قانونية وتشريعية متزايدة، تهدف إلى ضمان أمن البيانات وحقوق الأفراد، ومساءلة الأطراف المتسببة في أي خرق أمني أو تسريب معلوماتي.

تنبع هذه التحديات من عدة عوامل، أبرزها التطور السريع للتقنيات مقارنةً بوتيرة تحديث القوانين، وتعدد مصادر التهديدات المعلوماتية، وصعوبة التوفيق بين حرية المعلومات وحماية الخصوصية، فضلاً عن التداخل في الاختصاصات القضائية بين الدول بسبب الطبيعة العابرة للحدود للجرائم الإلكترونية.

#### **أولا: غياب أو تأخر التشريعات الوطنية :**

في العديد من البلدان، لا تزال الأطر القانونية المتعلقة بأمن المعلومات في مراحلها الأولى، أو غير محدثة لمواكبة التطورات التكنولوجية. وهذا التأخر يخلق فراغاً قانونياً تستغله جهات خبيثة للقيام بعمليات اختراق أو تسريب دون مواجهة عقوبات رادعة. كما أن بعض التشريعات تكون عامة وغامضة، ولا تفصل في مسائل تقنية دقيقة مثل حماية كلمات المرور أو تشفير البيانات أو شروط استخدام أنظمة المراقبة.

#### **ثانيا: تعقيد الجرائم الإلكترونية وصعوبة الإثبات :**

تُعد الجرائم المتعلقة بالمعلومات من أكثر الجرائم تعقيداً على المستوى القانوني، إذ يصعب إثبات وقوعها، أو تحديد مرتكبيها، خصوصاً عندما تُنفذ من خارج الدولة أو من خلال شبكات افتراضية مشفّرة. وتواجه الجهات القضائية صعوبة في تتبع الأدلة الرقمية أو إثبات النية الجنائية، ما يؤدي في أحيان كثيرة إلى إفلات الجناة من العقاب.

#### **ثالثا: حماية الخصوصية في مقابل الأمن:**

يمثل التوفيق بين حماية أمن المعلومات من جهة، وحقوق الأفراد في الخصوصية من جهة أخرى، تحدياً قانونياً مستمراً. ففي الوقت الذي تحتاج فيه المؤسسات الخدمية إلى مراقبة الأنظمة والشبكات بشكل دائم لحماية البيانات، قد تُتّهم بانتهاك خصوصية الموظفين أو المستخدمين إذا لم تكن هناك ضوابط قانونية واضحة تنظم هذا الأمر. وهنا يتجلى دور التشريعات في إيجاد توازن دقيق بين المتطلبات الأمنية والحريات الفردية.

#### **رابعا: التحديات ذات الطابع الدولي:**

بما أن الجريمة السيبرانية تتجاوز الحدود الوطنية، فإن غياب اتفاقيات دولية فعالة لتبادل المعلومات والمساعدة القضائية بين الدول يشكل عقبة كبيرة أمام ملاحقة المجرمين السيبرانيين. فمثلاً، قد يتم اختراق نظام مؤسسة خدمية جزائرية من قبل جهة موجودة في دولة لا تربطها بالجزائر اتفاقيات تسليم المجرمين أو تعاون أمني إلكتروني، مما يصعب عملية التحقيق ويعرقل الإجراءات القانونية.

#### **خامسا: نقص الكوادر القضائية المتخصصة**

تتطلب القضايا المتعلقة بحماية المعلومات وجود قضاة، محامين، وخبراء تقنيين على دراية بالجوانب التقنية والتشريعية لهذه القضايا. لكن الواقع يشير إلى نقص واضح في هذا النوع من الكفاءات في العديد من الدول النامية، ما يؤدي إلى ضعف مخرجات القضاء في مثل هذه الملفات، وتفاقم التهديدات المعلوماتي.

ومن الحلول لتجاوزها:

* سنّ تشريعات واضحة ومفصلة تغطي جميع جوانب أمن المعلومات والجرائم الإلكترونية.
* تحديث القوانين بشكل دوري لمواكبة تطورات التكنولوجيا وأساليب الهجوم الحديثة.
* إنشاء هيئات وطنية متخصصة في الأمن السيبراني تُمنح صلاحيات رقابية وقضائية.
* تعزيز التعاون الإقليمي والدولي من خلال اتفاقيات تبادل البيانات والتحقيق المشترك.
* تكوين القضاة والمحققين في مجال الأدلة الرقمية والجريمة المعلوماتية.

**المطلب الثالث: سبل حماية امن المعلومات في المؤسسات الخدمية**

**الفرع الأول : الأساليب التقنية )التشفير،أنظمة كشف التسلل،إدارة الوصول)**

في العصر الرقمي الراهن، أصبحت المعلومات أحد الأصول الاستراتيجية الأكثر حساسية، لا سيما في المؤسسات الخدمية التي تتعامل يوميًا مع بيانات شخصية ومالية وصحية لملايين الأفراد. ونظرًا لتزايد الهجمات الإلكترونية، أضحت **تقنيات حماية البيانات** ضرورة قصوى، وفي مقدمتها **التشفير (Encryption)**، الذي يُعد من أقوى الأدوات التقنية لضمان سرية وسلامة البيانات، سواء أثناء تخزينها أو نقلها عبر الشبكات.

#### **أولًا: التشفير**

**1-مفهوم التشفير:**

التشفير هو عملية تحويل البيانات من صيغة مفهومة إلى صيغة غير قابلة للقراءة دون مفتاح أو رمز خاص يُستخدم لفك الشيفرة. الهدف من التشفير هو حماية المعلومات من الوصول غير المصرح به، سواء من داخل المؤسسة أو من خارجها.

يعتمد التشفير على خوارزميات رياضية معقدة، تُصنف عادةً إلى نوعين رئيسيين:

**التشفير المتماثل** : حيث يُستخدم نفس المفتاح للتشفير وفك التشفير. ومن أشهر خوارزمياته: AES (Advanced Encryption Standard)

**التشفير غير المتماثل (Asymmetric Encryption)**: ويُستخدم فيه مفتاحان مختلفان (مفتاح عام ومفتاح خاص). أشهر تطبيقاته هو نظام[[17]](#footnote-17) RSA

#### **2- أهمية التشفير في حماية البيانات**

يلعب التشفير دورًا محوريًا في حماية البيانات الحساسة، لا سيما في المجالات التالية:

* **حماية الاتصالات الإلكترونية**: مثل البريد الإلكتروني، والرسائل النصية، والمكالمات الصوتية، حيث يضمن أن المراسلات لا يُمكن اعتراضها وفهمها.
* **تأمين المعاملات المالية**: كما هو الحال في خدمات الدفع الإلكتروني، حيث تُمكّن تقنيات التشفير من حماية بيانات البطاقات البنكية والمعاملات.
* **تخزين آمن للبيانات**: تمنع تقنيات التشفير الاطلاع غير المصرح به على البيانات المُخزنة، سواء على الأقراص الصلبة أو على خوادم السحابة.
* **الامتثال القانوني**: تساعد تقنيات التشفير المؤسسات على الالتزام بالقوانين المتعلقة بحماية البيانات مثل اللائحة العامة لحماية البيانات الأوروبية.

#### **3- تقنيات أخرى لحماية البيانات**

إلى جانب التشفير، هناك عدة تقنيات تُستخدم لحماية البيانات من التهديدات الخارجية والداخلية، ومن أبرزها :

* **النسخ الاحتياطي** : يُعد من أهم وسائل الحماية لضمان استعادة البيانات في حال الفقد أو التلف أو الهجوم، خاصة في حالات هجمات الفدية.
* **إخفاء البيانات** : يُستخدم لحماية البيانات الحساسة عند استخدامها في بيئات التطوير أو الاختبار، من خلال استبدال القيم الأصلية بقيم زائفة تُشبهها في البنية.
* **تقنيات تجزئة البيانات** : وهي آلية لتحويل البيانات إلى سلسلة مشفرة ثابتة الطول، تُستخدم للتحقق من سلامة البيانات وكشف أي تعديل غير مصرح به.
* **التحكم في الوصول** : يُمكّن المؤسسات من تحديد من يمكنه الوصول إلى أي نوع من البيانات، وفقًا للصلاحيات والوظائف.
* **التدقيق والمراقبة** : من خلال تتبع جميع العمليات التي تتم على البيانات، ما يسمح باكتشاف أي نشاط مشبوه أو غير اعتيادي.[[18]](#footnote-18)

**ثانيا: أنظمة كشف التسلل:**

في ظل تصاعد حجم التهديدات السيبرانية، لم تعد حماية محيط الشبكات والمعلومات مقتصرة على الجدران النارية والتشفير، بل أصبح من الضروري تبني أدوات أكثر ذكاءً وقدرة على كشف التهديدات عند حدوثها، والتفاعل السريع معها. وتُعد **أنظمة كشف التسلل (Intrusion Detection Systems - IDS)** و**الاستجابة للحوادث (Incident Response)** من الركائز الأساسية لأي بنية أمن معلومات متكاملة، خاصة داخل المؤسسات الخدمية التي تعتمد على توفر الخدمة بشكل مستمر وثقة المستخدمين.

أنظمة كشف التسلل هي أدوات برمجية أو مادية تُستخدم لرصد النشاطات غير المصرح بها أو المشبوهة داخل شبكة المعلومات أو الأنظمة. تهدف هذه الأنظمة إلى:[[19]](#footnote-19)

**تحليل حركة المرور** بحثًا عن أنماط هجوم معروفة.

**تنبيه المسؤولين** عن الأمن بمجرد اكتشاف تهديد محتمل.

**تقديم تقارير مفصلة** عن أنواع التهديدات ومصادرها.

**تصنيف أنظمة :**

**أنظمة قائمة على الشبكة** : تراقب حركة البيانات عبر الشبكة.

**أنظمة قائمة على المضيف** : تراقب الأنشطة داخل الأجهزة نفسها، مثل الدخول غير المصرح به أو التعديل في ملفات النظام[[20]](#footnote-20).

كما تنقسم حسب طريقة الكشف إلى:

**كشف قائم على التوقيع** : يكتشف التهديدات المعروفة.

**كشف قائم على السلوك (Anomaly-based)**: يكتشف أنشطة غير طبيعية تشير إلى تهديد محتمل حتى لو كان جديدًا.

#### **-الاستجابة للحوادث:**

#### تُعرف الاستجابة للحوادث على أنها مجموعة من الإجراءات المُنظمة التي تُتخذ للتعامل مع الحوادث الأمنية عند وقوعها، بهدف تقليل آثارها السلبية، ومنع تكرارها. تشمل عملية الاستجابة للحوادث المراحل التالية:

**التحضير** : وضع خطة مسبقة وتدريب الفرق المختصة.

**التحديد** : تحديد ما إذا كان النشاط يشكل تهديدًا فعليًا.

**الاحتواء** : منع انتشار التهديد إلى بقية النظام.

**القضاء** : إزالة مصدر التهديد من النظام.

**الاسترداد** : إعادة النظام إلى حالته الطبيعية.

**الدروس المستفادة** : توثيق ما حدث لتحسين الأداء في المستقبل.

تقوم العديد من المؤسسات الكبيرة بتأسيس **فِرق استجابة للحوادث ,**تكون مهمتها التنسيق الكامل للتعامل مع الهجمات السيبرانية.

#### **- أهمية الاستجابة للحوادث في المؤسسات الخدمية:**

تلعب هذه الأدوات دورًا بالغ الأهمية في المؤسسات الخدمية، خاصة تلك التي تقدم خدمات حيوية كالصحة، التعليم، والبريد، نظرًا للآثار الوخيمة التي قد تترتب عن توقف الخدمة أو تسرب البيانات.

تُمكن أنظمة كشف التسلل من رصد محاولات الدخول غير المصرح به إلى الحسابات البريدية أو قواعد البيانات بينما تُقلل الاستجابة السريعة للحوادث من مدة انقطاع الخدمة وتمنع تفاقم الخسائر.

### **ثالثا: إدارة الوصول والصلاحيات**

في إطار حماية نظم المعلومات بالمؤسسات الخدمية، لا يمكن الاكتفاء فقط بتقنيات التشفير أو أنظمة كشف التسلل، بل تبرز ضرورة ضبط من يمكنه الوصول إلى المعلومات وكيف ومتى ولماذا، وهي ما يُعرف بـ **إدارة الوصول والصلاحيات** . فغياب هذه المنظومة يُعتبر أحد أكبر التهديدات التي قد تؤدي إلى تسرب البيانات أو التلاعب بها، حتى من قبل المستخدمين الشرعيين.[[21]](#footnote-21)

#### **1-مفهوم إدارة الوصول والصلاحيات**

تُشير إدارة الوصول إلى مجموعة السياسات والإجراءات والضوابط التقنية التي تهدف إلى التحكم في من يُسمح له بالوصول إلى نظم المعلومات، وعلى أي مستوى، وفي أي ظروف. وتتضمن هذه الإدارة.

**المصادقة** : التحقق من هوية المستخدم.

**التفويض** : تحديد ما يُسمح للمستخدم بالقيام به بعد المصادقة.

**التتبع** : تسجيل ومراقبة الأنشطة التي يقوم بها المستخدمون.

ويُعتبر هذا النظام بمثابة البوابة الأولى أمام كل محاولة استخدام أو تعديل أو حذف للمعلومات الحساسة.[[22]](#footnote-22)

#### **2-نماذج التحكم في الوصول:**

توجد عدة نماذج تعتمدها المؤسسات لتنظيم إدارة الصلاحيات، نذكر من أبرزها:

**التحكم الإجباري في الوصول** : تُحدد صلاحيات الوصول من قبل النظام بناءً على تصنيفات أمنية صارمة، ويُستخدم غالبًا في البيئات الحكومية أو العسكرية.

**التحكم القائم على الدور** : يُمنح المستخدمون صلاحيات بناءً على أدوارهم الوظيفية داخل المؤسسة، وهو الأكثر استخدامًا في المؤسسات الخدمية.

**التحكم القائم على السياسة** : يُتيح تحديد الوصول بناءً على مجموعة من السياسات التي قد تشمل الوقت، الموقع، نوع الجهاز، وغيرها.

**التحكم القائم على السمات** : يُمنح الوصول بناءً على خصائص المستخدم والسياق، ويُستخدم في الأنظمة الذكية والحوسبة السحابية.

#### **3- أهمية إدارة الصلاحيات في المؤسسات الخدمية:**

تُعد إدارة الوصول والصلاحيات حجر الزاوية في حماية المعلومات داخل المؤسسات الخدمية مثل البريد، التعليم، الصحة، والقطاع البنكي. ومن بين أبرز مزايا هذا النظام.

**تقليل فرص تسرب البيانات** من خلال الحد من عدد الأشخاص المسموح لهم بالوصول إلى المعلومات الحساسة.

**الحد من الأخطاء البشرية أو السهو** التي قد تحدث بسبب وصول غير مبرر لبعض الموظفين إلى بيانات لا تخصهم.

**تحقيق الامتثال للضوابط القانونية والتنظيمية** مثل قوانين حماية البيانات **تعزيز مبدأ "الحد الأدنى من الامتيازات" (Least Privilege)**، أي أن كل موظف يحصل فقط على الصلاحيات الضرورية لأداء عمله.

**تيسير عمليات التدقيق والتحقيق في الحوادث** بفضل وجود سجلات واضحة تُظهر من قام بماذا ومتى.

يُمنع على الموظفين العاديين الوصول إلى بيانات المستخدمين دون تصريح إداري.

يتم تطبيق نموذج لتقسيم صلاحيات الموظفين حسب القسم والوظيفة.[[23]](#footnote-23)

يُراقب النظام آليًا محاولات الدخول غير المصرح بها، ويُوقف الحسابات المشبوهة تلقائيًا.

**الفرع الثاني: السياسات و الإجراءات الإدارية لحماية امن المعلومات في المؤسسات الخدمية**

### **أولا: تطوير سياسات وإجراءات أمن المعلومات**

سياسة أمن المعلومات هي الإطار التنظيمي الذي يعكس التوجه العام للمؤسسة نحو حماية مواردها المعلوماتية، وتُعد من العناصر الأساسية التي تضمن استمرارية العمل بأمان وكفاءة. وفي المؤسسات الخدمية .

تتجسد سياسات أمن المعلومات في مجموعة من القواعد والخطوط العريضة التي تحدد كيف تُدار المعلومات، من يمكنه الوصول إليها، وكيفية حمايتها من التهديدات الداخلية والخارجية. يبدأ تطوير هذه السياسات بتحديد الأهداف الأساسية لأمن المعلومات، وهي: **السرية، السلامة، والتوافر**. وبناءً على ذلك، يُصاغ هيكل متكامل يشمل.

تصنيف المعلومات حسب حساسيتها.

تحديد مستويات الوصول والصلاحيات.

وضع آليات للتشفير والنسخ الاحتياطي.

إنشاء خطة للاستجابة للحوادث والطوارئ.

عملية تطوير السياسات تمر بمراحل أساسية، تبدأ بتقييم المخاطر الأمنية، ثم التشاور مع مختلف الأقسام المعنية داخل المؤسسة، وصولًا إلى الصياغة الرسمية والتطبيق الفعلي. ومن بين أبرز التحديات التي تواجهها المؤسسات الخدمية عند صياغة هذه السياسات: ضعف الثقافة الأمنية لدى الموظفين، تقلب التهديدات السيبرانية، وضغوط الامتثال للقوانين المحلية والدولية.

تتميز السياسات الفعّالة بكونها مرنة وقابلة للتحديث، كما يجب أن تكون مكتوبة بلغة واضحة، متاحة لجميع العاملين، ومُدعّمة بإجراءات تفصيلية تضمن التنفيذ الصحيح. من جهة أخرى، تضمن **إجراءات أمن المعلومات (Security Procedures)** تطبيق تلك السياسات على أرض الواقع عبر تعليمات محددة، مثل كيفية إعداد كلمات السر، آليات مراقبة الدخول إلى الأنظمة، وضوابط استخدام البريد الإلكتروني المهني.[[24]](#footnote-24)

### **ثانيا : التوعية والتدريب الأمني للعاملين في المؤسسات الخدمية (كوادر بشرية متخصصة(**

في عالم تتزايد فيه التهديدات السيبرانية بشكل غير مسبوق، لم يعد تأمين نظم المعلومات في المؤسسات الخدمية يعتمد فقط على الحلول التقنية، بل أصبح الاستثمار في العامل البشري عاملاً حاسمًا في تحقيق الأمن المعلوماتي الشامل. فحتى أقوى النظم عرضة للخطر إذا ما استُخدمت من قبل موظفين يفتقرون إلى الثقافة الأمنية الأساسية. من هنا، تبرز أهمية التوعية والتدريب الأمني كأحد الأعمدة المركزية في البنية التحتية لأمن المعلومات، خصوصًا في مؤسسات خدمية حساسة.

التوعية الأمنية تعني تزويد جميع العاملين، من أعلى الهرم الإداري إلى أصغر الموظفين، بالمعرفة الأساسية حول كيفية حماية المعلومات، والتصرف الصحيح في مواجهة الحوادث الأمنية، وتجنب السلوكيات الخطرة، كفتح الروابط المشبوهة أو استخدام كلمات مرور ضعيفة. أما التدريب الأمني فيذهب إلى ما هو أعمق، حيث يشمل برامج منتظمة وممنهجة تستهدف تنمية الكفاءات الفنية والسلوكية، وتهيئة كوادر متخصصة قادرة على الاستجابة بفعالية لأي اختراق أو محاولة تسلل.

يشمل التدريب الأمني ثلاث مستويات أساسية:[[25]](#footnote-25)

**التدريب العام**: موجه لكل الموظفين، ويتضمن توجيهات أساسية حول أمن البريد الإلكتروني، إدارة كلمات السر، وتجنب الهندسة الاجتماعية.

**التدريب المتخصص**: موجه للموظفين التقنيين ومسؤولي الأنظمة والشبكات، ويشمل تقنيات متقدمة في الحماية، تحليل الاختراقات، وأنظمة كشف التسلل.

**التدريب الإداري**: يخص القيادات وصناع القرار، ويركز على فهم السياسات الأمنية، إدارة الأزمات، والتعامل مع الإعلام في حال حصول خروقات.

وتتجلى أهمية هذا الجانب بشكل أكبر في المؤسسات الخدمية ذات الطابع الجماهيري، أين يكون الخطأ البشري أكثر احتمالية، وحيث يمكن أن تؤدي غفلة بسيطة إلى تسريب بيانات آلاف المستخدمين أو توقف الخدمات بشكل كامل. في هذا السياق، يُعتبر تنظيم دورات دورية، وورش عمل، ومحاكاة لهجمات إلكترونية واقعية من أنجع الطرق لتعزيز الجاهزية الأمنية للمؤسسة.

كما يُستحسن تبني أسلوب "التدريب حسب الوظيفة"، أي مواءمة المادة التدريبية مع المهام اليومية للمستخدم، مما يُكسبه مهارات واقعية مباشرة التطبيق. ويمتد تأثير التوعية الأمنية إلى سلوكيات الموظفين حتى خارج مكان العمل، مما يخلق ثقافة أمنية مستدامة ترفع من مستوى التحصين العام للمؤسسة.

أخيرًا، لا يجب النظر إلى التوعية والتدريب الأمني كتكلفة، بل كاستثمار طويل الأمد يعود بالنفع على سلامة المؤسسة، ويحمي سمعتها، ويعزز من ثقة المستخدمين بخدماتها.

### **الفرع الثالث : دور القوانين والتشريعات في حماية البيانات والمعلومات**

تُعد القوانين والتشريعات المتعلقة بحماية البيانات والمعلومات إحدى الركائز الأساسية التي تضمن عدم تعرض المعلومات الحساسة داخل المؤسسات الخدمية مثل "بريد الجزائر" للتهديدات أو التسربات غير المصرح بها. فقد أصبحت حماية البيانات في عصر التكنولوجيا الرقمية من الأولويات العالمية، بسبب تزايد الانتهاكات والاختراقات الإلكترونية التي تهدد خصوصية الأفراد وأمن المؤسسات.

القوانين المتعلقة بحماية البيانات تلعب دورًا محوريًا في وضع إطار قانوني يُلزم المؤسسات بتبني سياسات أمنية صارمة لضمان الحفاظ على سرية المعلومات وحمايتها من الاختراقات. وعلى المستوى الدولي، تُعد **اللائحة العامة لحماية البيانات**  في الاتحاد الأوروبي واحدة من أبرز التشريعات التي فرضت معايير عالية لحماية البيانات الشخصية، وهي ملزمة لجميع المؤسسات التي تتعامل مع بيانات المواطنين الأوروبيين، بغض النظر عن مكان تواجدها. تُحدد هذه اللائحة مبادئ أساسية، منها: الشفافية في جمع البيانات، الحق في الوصول والتصحيح، وأهمية الحصول على موافقة مسبقة لجمع البيانات.[[26]](#footnote-26)

وفي السياق الجزائري، تم إصدار **قانون حماية المعلومات الشخصية** في إطار تحسين التشريعات الوطنية المتوافقة مع المعايير العالمية. يتضمن هذا القانون مبادئ أساسية تشترط حماية البيانات الشخصية للمواطنين، وتشمل عناصر مثل فرض رقابة على استخدام البيانات الشخصية، وتحديد صلاحيات الجهات التي تستطيع الوصول إلى هذه البيانات. كما يتطلب القانون من المؤسسات وضع تدابير أمان وقائية، مثل التشفير، للتحكم في الوصول إلى البيانات وحمايتها من الاستخدام غير المشروع.

ومن جهة أخرى، يُعتبر **قانون الجرائم الإلكترونية** أداة قانونية هامة في مواجهة التهديدات الإلكترونية، حيث يحدد عقوبات شديدة على الأفراد أو المؤسسات التي تتورط في ارتكاب جرائم إلكترونية مثل القرصنة، سرقة البيانات، أو نشر البرمجيات الخبيثة. ويعمل هذا القانون على تعزيز الدور الرقابي للأجهزة المعنية، مثل هيئة حماية المعلومات الشخصية، في مراقبة تنفيذ التزامات حماية البيانات في المؤسسات.

تُسهم هذه التشريعات بشكل كبير في تحقيق **الامتثال القانوني**، وهو أحد الأبعاد الأساسية لإدارة أمن المعلومات داخل المؤسسات الخدمية. فالمؤسسات التي تلتزم بتطبيق هذه القوانين لا تحمي فقط معلومات العملاء والمستخدمين، بل تحمي أيضًا نفسها من العقوبات القانونية والمالية التي قد تترتب على فشلها في الالتزام بالمعايير القانونية.

من جهة أخرى، تلعب التشريعات دورًا في فرض الشفافية والمساءلة داخل المؤسسة، حيث يُلزم القانون المؤسسات بتوضيح كيفية جمع وتخزين واستخدام البيانات، إضافة إلى فرض قيود صارمة على التفاعل مع الأطراف الخارجية (مثل الموردين أو شركاء الأعمال) في ما يخص البيانات الحساسة.

في هذا الإطار، تتطلب التشريعات الحديثة من المؤسسات أن تتبنى **استراتيجيات حماية البيانات**، بما في ذلك تقنيات التشفير، والمراقبة المستمرة، وتنفيذ خطط الطوارئ للاستجابة للحوادث. هذا إلى جانب التدريب المستمر للموظفين، لضمان أنهم على دراية بكيفية حماية البيانات من التسربات، وتجنب التصرفات غير الآمنة التي قد تعرض البيانات للسرقة أو الاختراق.

بالتالي، تشكل القوانين والتشريعات المتعلقة بحماية البيانات المكون الأساسي لضمان حماية المعلومات في المؤسسات الخدمية، وفي تعزيز الثقة بين المؤسسة والعملاء. كما توفر هذه التشريعات حوافز للمؤسسات للتحسين المستمر لآليات الأمان، وتهدف في المجمل إلى إنشاء بيئة آمنة تدعم نمو الأعمال وتدعم الابتكار دون المساس بالحقوق الفردية للمستخدمين.

**المبحت التاني : الدراسات السابقة**

سوف نتناول في هدا المبحث أهم الدراسات السابقة, فقد تطرقنا الى تقسيمه الى ثلاث مطالب, والمطلب الأول كان حول الدراسات باللغة العربية و المطلب الثاني فكان حول الدراسات باللغة الأجنبية , أما المطلب الثالث فكان مقارنة بين الدراسات السابقة والدراسة الحالية.

**المطلب الأول: الدراسات باللغة العربية**

**الدراسة الأولى : بدودة مريم دراسة بعنوان : دور أمن المعلومات في تحقيق الميزة التنافسية لفروع شركة سوناطراك بالجزائر"، 2021**

هدفت هذه الدراسة إلى تحليل مدى تأثير تطبيق ممارسات أمن المعلومات داخل فروع شركة سوناطراك على تحقيق الميزة التنافسية. واعتمدت على المنهج الوصفي التحليلي، حيث تم توزيع استبانة على عينة عشوائية مكونة من 110 موظفًا، وتم تحليل البيانات باستخدام برنامج SPSS19. وقد طرحت الدراسة إشكالية محورية تمثلت في التساؤل عن الدور الذي يلعبه أمن المعلومات في دعم القدرة التنافسية للفروع، وسعت إلى تحديد العلاقة بين درجة تطبيق أمن المعلومات ومستوى الأداء التنافسي. توصلت الدراسة إلى أن فروع الشركة تطبق أمن المعلومات بمستوى مرتفع، كما أظهرت وجود علاقة ارتباط موجبة متوسطة وذات دلالة إحصائية بين أمن المعلومات والميزة التنافسية، مما يعكس أهمية تبني سياسات حماية رقمية فعّالة كعامل داعم للتفوق في بيئة الأعمال. وقد أوصت الدراسة بضرورة مواصلة تطوير استراتيجيات أمن المعلومات وتعزيز الوعي المؤسسي بأهميتها، لما لذلك من أثر مباشر في تحسين الأداء وتعزيز استدامة التميز في السوق.

**الدراسة الثانية : أحمد محمد حمد البركي والمعنونة بـ "واقع تطبيق متطلبات نظم إدارة أمن المعلومات المتوافقة مع المواصفة ISO/IEC 27001 : سنة 2020**

هدفت الدراسة إلى التعرف على مدى الالتزام بتطبيق متطلبات نظام إدارة أمن المعلومات من حيث السياسات والتقنيات والتنظيم والموارد البشرية، وذلك عبر استبيان شمل موظفي إدارات تقنية المعلومات. أظهرت النتائج أن مستوى التطبيق كان متوسطًا، مع تفاوت واضح حسب المتغيرات الديموغرافية والوظيفية للعاملين. وأوصت الدراسة بضرورة إنشاء إدارات مختصة بأمن المعلومات داخل المصارف، وتكثيف برامج التوعية والتدريب لتعزيز ثقافة الحماية الرقمية في البيئة المصرفية.

**الدراسة الثالثة :**

**قدور مقراني مذكرة ماستر بعنوان "تقييم مدى مساهمة أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم المعلومات – دراسة حالة مؤسسة اتصالات الجزائر". 2016**

هدفت هده الدراسة إلى قياس مساهمة أمن نظام المعلومات في الحد من المخاطر التي تهدد استمرارية الأداء المعلوماتي داخل المؤسسة. استندت الدراسة إلى المنهج الوصفي، ووزعت استبيانًا استرجعت منه 90 استمارة، بنسبة استجابة بلغت 90%. خلصت النتائج إلى أن وجود سياسات أمنية واضحة يساهم في تقليل المخاطر المرتبطة بالمكونات المادية والبرمجية للنظام، كما أن إشراك العنصر البشري في تنفيذ هذه السياسات يعزز فعالية الأمن المعلوماتي. رغم أن نظام المعلومات بالمؤسسة يحتوي على جوانب إيجابية، إلا أن الباحثة ترى أنه لا يزال دون المستوى المطلوب مقارنة بمكانة المؤسسة في قطاع الاتصالات بالجزائر. وقد خلصت إلى أن إشراك العنصر البشري وتطبيق الإجراءات الأمنية المناسبة يسهم بشكل ملحوظ في حماية الأنظمة وضمان استمرارية العمل المعلوماتي.

**الدراسة الرابعة حمودي كاهنة مذكرة ماستر بعنوان "نظام أمن المعلومات في الجزائر: دراسة حالة بلدية سوق الإثنين – ولاية تيزي وزو (2014-2017)"**

تهدف الدراسة إلى تسليط الضوء على واقع نظام أمن المعلومات في الإدارة المحلية الجزائرية، ومدى التزام بلدية سوق الإثنين بتطبيق آليات الحماية المعلوماتية. تؤكد الدراسة أن المعلومة تمثل الهدف الأساسي الذي يُثبت صحة الفرضيات، لذا يتطلب استخدامها الميداني التحقق من قدرتها على تجاوز عرقلة الاستخدام، وذلك عبر نظام معلومات متكامل يضمن الرقابة الشاملة والحفاظ على سلامة البيانات. تختلف نظم المعلومات باختلاف مجالات استخدامها وبيئتها، ولهذا تتطلب دراسة معمقة لمكوناتها لضمان التوافق بين المعلومات وبيئتها. مع تسارع الحاجة إلى كسب المعلومات وحمايتها، لجأت المؤسسات إلى أنظمة أمن المعلومات لتفادي الاختلاس الإلكتروني وتأمين السرية في التخزين والإرسال، مستندة إلى المعايير الدولية مثل نظام ISO 150. وقد أولت الجزائر اهتمامًا خاصًا لتأمين المعلومات داخل مؤسساتها الإدارية من خلال سن قوانين لمكافحة القرصنة الإلكترونية والجرائم السيبرانية، التي تهدد سلامة العمل الإداري. ورغم ذلك، كشفت الدراسة عن وجود قصور في تطبيق النظم الأمنية ببلدية سوق الإثنين بسبب ضعف الإمكانيات التقنية والبشرية، مما يعرض البيانات لمخاطر متعددة.

**المطلب الثاني: الدراسات بالغة الاجنبية**

1. **Sarah Ewuga, Zainab Egieya, et al. (2023) – A study on the implementation of ISO 27001 Information Security Management System (ISMS) in the banking sector**

سلطت هذه الدراسة الضوء على أهمية تطبيق نظام إدارة أمن المعلومات ISO 27001 في القطاع المصرفي، حيث ركزت على كيفية مساهمة هذا المعيار في تعزيز حماية البيانات داخل المؤسسات المالية. وقد بينت النتائج أن اعتماد ISO 27001 ساهم بشكل كبير في تحسين إدارة المخاطر، ورفع وعي الموظفين، وتعزيز ثقافة الأمن الداخلي، وكل ذلك دعم بشكل مباشر حماية البيانات الحساسة واستمرارية العمليات المصرفية.

1. **Mahsa Mohseni (2023) – A study on the compliance of an Iranian bank with ISMS requirements**

استكشفت هذه الدراسة مدى امتثال أحد البنوك الإيرانية لمتطلبات نظام إدارة أمن المعلومات (ISMS). واستنادًا إلى مقابلات مع موظفي قسم تقنية المعلومات، كشفت الدراسة عن تحديات رئيسية في عملية التنفيذ، مثل نقص التدريب، وانخفاض الوعي الأمني، والمقاومة الداخلية للتغيير. واختتمت الدراسة بالتأكيد على ضرورة بناء القدرات وتنفيذ برامج توعوية لتعزيز جاهزية المؤسسة لاعتماد ISMS بشكل فعال.

1. **Rudy Aryanto (2014) – Designing a governance model for information security systems in banks based on the COBIT 4.1 framework and integrated with ISO 27001 standard**s

هدفت هذه الدراسة إلى تصميم نموذج حوكمة لنظم أمن المعلومات في البنوك، اعتمادًا على إطار عمل COBIT 4.1 وبالدمج مع معايير ISO 27001. وقد استخدمت الدراسة نموذج النضج لتقييم الوضع الأمني للمؤسسات المالية، وكشفت عن عدة ثغرات أمنية. وأوصت النتائج باعتماد تدابير رقابة منظمة لتحسين حوكمة تقنية المعلومات وضمان توافقها مع الأهداف الإستراتيجية للمؤسسة.

**المطلب الثالث: مقارنة بين الدراسة الحالية والدراسات السابقة**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **الدراسة الحالية** | **بدودة مريم** | **البركي** | **مقراني** | **حمودي كاهنة** | **Ewuga et al.** | **Aryanto** | **Mohseni** | **وجه المقارنة** |
| الجزائر | الجزائر | ليبيا | الجزائر | الجزائر | نيجيريا | إندونيسيا | إيران | **بلد الدراسة** |
| مؤسسة خدمية | شركة نفط وطنية (سوناطراك) | مصارف | اتصالات الجزائر | بلدية | مصارف | مصارف | مصرف | **نوع**  **المؤسسة** |
| نظم أمن المعلومات في المؤسسات الخدمية | علاقة أمن المعلومات بالميزة التنافسية | تطبيق ISO/IEC 27001 | دور الأمن في الحد من المخاطر | واقع أمن المعلومات في بلدية | ISO 27001 وأثره على الأمان المصرفي | حوكمة أمن المعلومات | تحديات تطبيق ISMS | **الموضوع الرئيسي** |
| تحليل التحديات وتقديم حلول | قياس العلاقة مع الميزة التنافسية | قياس الالتزام بالمعايير | تقليل المخاطر المعلوماتية | فحص واقع النظام في البلدية | قياس فعالية ISO 27001 | بناء نموذج حوكمة | تحليل التحديات الداخلية | **الهدف**  **الأساسي** |
| وصفي تحليلي | وصفي تحليلي | وصفي ميداني | وصفي تحليلي | تحليل وصفي ميداني | كمي تحليلي | نمذجة حوكمة | مقابلات وتحليل كيفي | **المنهج المستخدم** |
| استبيان وتحليل محتوى | استبيان | استبيان | استبيان | تحليل وصفي | تحليل نتائج معيار ISO | مصفوفة نضج الحوكمة | مقابلات | **أداة الدراسة** |
| ضرورة تحسين الأنظمة وتطبيق استراتيجيات حماية | علاقة إيجابية بين أمن المعلومات والميزة التنافسية | التطبيق متوسط ويحتاج تحسين | أمن المعلومات يقلل المخاطر | قصور في تطبيق النظام بالبلدية | ISO 27001 يحسن الأداء الأمني | الحوكمة تعزز الأمان الاستراتيجي | مقاومة التغيير تعيق التطبيق الفعال | **أهم النتائج** |

**التحليل** :

أوجه التشابه:

معظم الدراسات استخدمت المنهج الوصفي التحليلي.

ركزت جميع الدراسات على أهمية وجود سياسات أمنية فعالة والتدريب المستمر والوعي المعلوماتي.

تمحورت الدراسات الأجنبية حول المعايير الدولية (ISO 27001 وCOBIT)، وهو ما يُكسب دراستك قيمة إذا أدمجت تلك المرجعيات.

الاختلافات:

دراستي أوسع من حيث الأهداف، إذ تجمع بين المفاهيم النظرية، التحديات، الحلول العملية، والتوصيات التقنية والإدارية.

بعض الدراسات ركزت على علاقة أمن المعلومات بمجالات أخرى (مثل التنافسية – بدودة مريم)، بينما أنت تركّزين على التحديات والتحسينات داخليًا في المؤسسات الجزائرية.

القيمة المضافة

محلية السياق لكنها مفتوحة على ال.معايير العالمية.

اقتراح حلولًا عملية لتحسين نظم الأمن المعلوماتي، عكس بعض الدراسات التي توقفت عند التشخيص.

**خلاصة عامة للدراسات السابقة**

يتضح من خلال عرض الدراسات السابقة أن هناك قواسم مشتركة بين تجارب الدول المختلفة في موضوع أمن المعلومات، خاصة فيما يتعلق بتحديات التطبيق، ومنها:

* ضعف البنية التنظيمية والتقنية.
* قلة الوعي الأمني لدى الموظفين.
* نقص الكفاءات البشرية المؤهلة.

غياب الخطط الاستراتيجية وتقييم المخاطر كما تبرز أهمية المعايير الدولية، وعلى رأسها ISO 27001:2005، باعتبارها إطارًا شاملًا لتطبيق نظم إدارة فعالة لأمن المعلومات، مما يعزز من حماية البيانات وسير العمل في المؤسسات، وخاصة المصارف.

**خاتمة الفصل الأول**

حاولنا في هدا الفصل التعرف على مفهوم أمن نظم المعلومات في المؤسسات الخدمية، وقد تطرقنا في المبحث الأول الى مايلي: في البداية قمنا بتعريف نظم أمن المعلومات وشرح مكوناتها الأساسية مثل السرية، السلامة، والتوافر، التي تُعد من الركائز الجوهرية لضمان حماية البيانات والمعلومات. كما تناولنا أهمية أمن المعلومات في المؤسسات الخدمية التي تعتمد بشكل كبير على البيانات الحساسة في تقديم خدماتها, ثم قمنا بالانتقال إلى التهديدات والمخاطر التي تواجه أمن المعلومات، حيث تم تقسيم هذه التهديدات إلى داخلية وخارجية، بما في ذلك الأخطاء البشرية، ضعف الوعي الأمني، الهجمات السيبرانية، الفيروسات، والاختراقات. كما تناولنا التحديات القانونية والتشريعية المتعلقة بحماية المعلومات، موضحين كيفية تأثير التشريعات المحلية والدولية على حماية البيانات، مع إشارة خاصة إلى اللائحة العامة لحماية البيانات .

تناولنا كذلك الأساليب التقنية لحماية أمن المعلومات، بدءًا من تقنيات التشفير وصولاً إلى أنظمة كشف التسلل والإستجابة للحوادث. وناقشنا أيضًا أهمية السياسات والإجراءات الإدارية في حماية البيانات، مع التركيز على دور التدريب الأمني والتوعية بين الموظفين أخيرًا، خلصنا إلى أن الأمن المعلوماتي في المؤسسات الخدمية، يتطلب استراتيجية متكاملة تشمل التكنولوجيا، السياسات الإدارية، والوعي البشري. لتحقيق حماية فعّالة للبيانات.

أمافي المبحث الثاني فقد تطرقنا الى الدراسات السابقة منها الدراسات العربية والأجنبية وقمنا أيضا بمقارنة هده الدراسات بالدراسة التي قمنا بها .

وسنتطرق في الفصل الثاني على الدراسة الميدانية التي أقيمت في مؤسسة بريد الجزائر .

**الفصل الثاني:**

**دراسة ميدانية**

**تمهيد :**

يُعتبر الفصل التطبيقي من أهم فصول المذكرة، إذ يُترجم الجانب النظري إلى واقع ملموس من خلال دراسة ميدانية تهدف إلى استقصاء واقع تطبيق نظم أمن المعلومات داخل المؤسسات الخدمية، وبالتحديد في مؤسسة بريد الجزائر. وقد تم اختيار هذه المؤسسة نظرًا لحساسيتها المعلوماتية، واعتمادها المتزايد على الأنظمة الإلكترونية في أداء مختلف عملياتها.

من خلال هذا الفصل، سيتم إبراز مدى وعي الموظفين بأهمية أمن المعلومات، والكشف عن مدى التزام الإدارة العليا بتوفير بيئة آمنة ومستقرة معلوماتيًا. كما سيتم ربط هذه النتائج بالسياق النظري الذي تم عرضه في الفصول السابقة، لتقديم رؤية شاملة حول موضوع الدراسة من الناحيتين النظرية والتطبيقية**.** وقد تم تسيم هدا الفصل الى مبحثين:

المبحث الأول: تقديم عام للمؤسسة وطرق وادوات الدراسة

المبحث الثاني: تحليل النتائج وإختبار الفرضيات

**المبحث الأول : تقديم عام للمؤسسة محل الدراسة ومنهجية وادوات الدراسة**

سنستعرض من خلال هذا المبحث تقديم عام للمؤسسة محل الدراسة، بالإضافة إلى إجراءات وأدوات الدراسة، وقد تم تقسيمه إلى مطلبين في المطلب الأول تقديم عام للمؤسسة محل الدراسة، والمطلب الثاني طرق الدراسة.

**المطلب الأول : تقديم عام للمؤسسة محل الدراسة**

**الفرع الأول : نشأة المديرية العامة لبريد الجزائر**

مؤسسة بريد الجزائر هي مؤسسة عمومية خدمية تأسست بعد إعادة هيكلة قطاع البريد وتكنولوجيات الإعلام والإتصال بموجب القانون 2000-03 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، بحيث تم إنشائها بموجب المرسوم 02/43 المؤرخ في 14 جانفي 2002، تتمتع بالشخصية المعنوية والإستقلال المالي وتتولى الخدمة العمومية بضمان تنفيذ السياسة الوطنية التطوير الخدمات البريدية والمالية في كامل التراب الوطني من خلال التكفل بنشاطات تسيير الأداءات وتجديد المؤسسات الأساسية المتصلة بذلك وتطويرها ( البريد والطرود البريد السريع الحساب البريدي الجاري، الطوابعية، دفتر التوفير والإحتياط وتتمثل في جمع الأموال لصالح صندوق التوفير والإحتياط التحويل الإلكتروني للأموال، الحوالات البريدية، الخدمات المصرفية الإلكترونية، تقع تحت وصاية الوزير المكلف بالبريد والمواصلات، ومقرها الإجتماعي حي الأعمال باب الزوار الجزائر " .

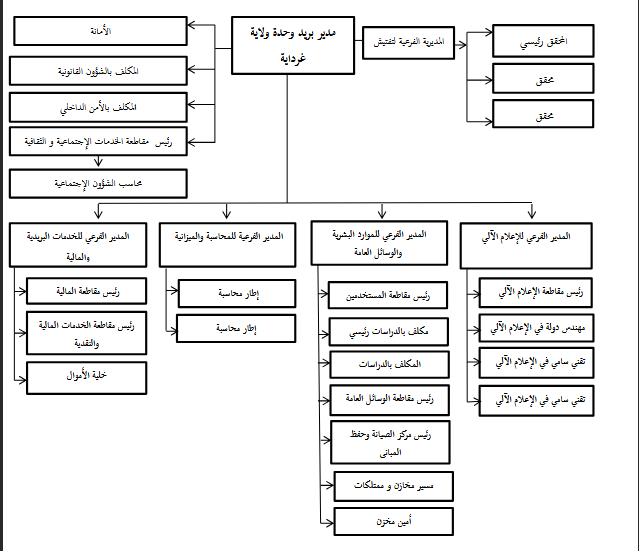
**الفرع الثاني : تعريف مديرية بريد الجزائر وحدة غرداية**

تقع مديرية بريد الجزائر وحدة ولاية غرداية في شارع العربي بن مهيدي طريق بني يزقن، حيث تضم 46 مكتب بريدي يتوزع على تراب الولاية حسب الكثافة السكانية، بالإضافة إلى 03 مراكز : وهي مركز الفرز الجهوي بغرداية، مركز الإيداع والتوزيع ، مركز الصيانة وحفظ المباني والسيارات.

**الفرع الثالث : هيكلة مديرية بريد الجزائر وحدة غرداية**

للهيكل التنظيمي المديرية بريد الجزائر وحدة غرداية دوراً هاما في تحديد المسؤوليات والمهام وتسهل عملية الرقابة داخلها وهو ما يعكسه التسيير والتنظيم الجيد لنشاطها والتنسيق بين مختلف وظائفها لتحقيق الأهداف الإستراتيجية، ولهذا سنقوم بعرض الهيكل التنظيمي المديرية بريد الجزائر وحدة غرداية في الشكل التالي :

**الشكل رقم (2-1) : يوضح الهيكل التنظيمي لمديرية الجزائر وحدة غرداية**



المصدر : وثائق مقدمة من طرف المؤسسة

**المطلب الثاني : طرق وأدوات الدراسة**

في هذا المطلب ستوضح الجوانب المنهجية للدراسة من منهج، يجتمع وعينة الدراسة، متغيرات الدراسة.

**الفرع الأول : منهج الدراسة**

بما أن الدراسة تهدف الى معرفة امن نظم المعلومات بمديرية بريد الجزائر وحدة غرداية فإن المنهج المناسب هو الوصفي ودراسة حالة، حيث اعتمدنا على المنهج الوصفي العرض الخلفية النظرية كونه يعد من أساليب البحث إذ يهتم بتحديد دقيق الأنشطة والأشياء والعمليات والأشخاص كما هي في الوقت الحاضر.

كما اعتمدنا على منهج دراسة الحالة في الجانب التطبيقي من خلال أداة الإستبيان، وقد تم توزيع إستبيانات في شكلها النهائي بغرض جمع بيانات تفيد في حق إشكالية الدراسة، حيث تم تجميعها ومن ثم تفريقها وتحليلها )Statistical Package for Social Sciences بإستخدام برنامج الحزمة الإحصائية للعلوم الإجتماعيةSPSS النسخة رقم (19) بهدف الوصول لدلالات ذات قيمة ومؤشرات ترجمت الى نتائج وتوصيات لدعم موضوع الدراسة .

**الفرع الثاني : مجتمع وعينة الدراسة**

يتكون مجتمع الدراسة من كل الموظفين التابعين بمديرية بريد الجزائر وحدة غرداية، الذين لهم علاقة بموضوع الدراسة موزعين كالآتي: إطار، إطار سامي عون تحكم عون تنفيذي، وبالنظر إلى توزيع مختلف الموظفين بالمديرية وحدة بريد الجزائر غرداية على العديد من المصالح، ونظرا لصغر حجم مجتمع الدراسة من الموظفين بها، فقد تم الإستعانة ببعض المكاتب البريدية الموزعة على تراب الولاية.وكان عدد مجتمع الدراسة 80 شخص.

**الجدول رقم (2\_1) :الإحصائية الخاصة باستمارة الاستبيان**

|  |  |  |
| --- | --- | --- |
| **الاستبيـان** |  | **البيان** |
| **النسبة** | **العدد** |
| **% 100** | **35** | **عدد الاستمارات الموزعة و المعلن عنها** |
| %14.29 | **05** | **عدد الاستمارات الملغاة** |
| %85.71 | **30** | **عدد الاستمارات الصالحة** |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

**الفرع الثالث : متغيرات الدراسة**

لدينا متغير وحيد وهو أمن نظم أمن المعلومات

**الفرع الرابع: ادوات الدراسة**

**ادوات جمع البيانات**

**الاستبيان :** تم الاعتماد في بحثنا على اداة الاستبيان كوسيلة لجمع البيانات والاستفادة منها , وقد خضع الاستبيان الى مجموعة من المراحل :

* اعداد استبيان اولي من أجل استخدامه في جمع البيانات.
* عرض الاستبيان على المشرفة من اجل اختبار مدى ملائمته لجمع البيانات.
* تعديل الاستبيان بشكل أولي حسب ماتراه المشرفة .
* عرض الاستبيان على الأساتذة المحكمين والأخذ بالملاحظات المقدمة.
* توزيع الاستبيان على جميع افراد العينة لجمع البيانات اللازمة .

واشتمل الاستبيان في مطلعه على رسالة وجهت إلى المبحوثين لحثهم على الإجابة بكل دقة وموضوعية، و قد تم تقسيمه إلى محورين:

* + **المحور الأول: البيانات الشخصية : العمر، المؤهل العلمي ، الوظيفة الحالية ، سنوات الخبرة.**
  + **المحور الثاني: يتضمن الابعاد التالية**:

**الجدول رقم (****2\_2) : عدد فقرات كل بعد**

|  |  |  |
| --- | --- | --- |
| عدد الفقرات | البعد | الرقم |
| 10 | **البيئة الإدارية لنظم أمن المعلومات** | 01 |
| **10** | **أساليب أمن نظم المعلومات** | 02 |
| **06** | **المعوقات التي تواجه تطبيق أمن المعلومات** | 03 |
| **26** | **المجموع** |  |

المصدر : من إعداد الطلبة اعتمادا على الاستبيان

**3 اختبار الثبات والصدق واختبار التوزيع الطبيعي**

**الفرع الأول: إختبار الثبات والصدق**

**أولًا: اختبار الثبات الداخلي لأداة الاستبيان (معامل كرونباخ ألفا)**

للتحقق من مدى **اتساق الفقرات الداخلية لكل محور** من محاور الاستبيان، تم استخدام **معامل الثبات كرونباخ ألفا (Cronbach’s Alpha)**، الذي يعد من أكثر الأساليب الإحصائية شيوعًا لقياس الثبات الداخلي في الدراسات الاجتماعية والإدارية. وقد تم الاعتماد على **برنامج التحليل الإحصائي SPSS**  لتحليل البيانات المستخلصة من عينة الدراسة والمقدرة بـ **30 استمارة**.

نتائج تحليل الثبات:

**الجدول رقم (2\_3) :نتائج تحليل الثبات**

|  |  |  |  |
| --- | --- | --- | --- |
| **البعد** | **عدد الفقرات** | **معامل كرونباخ ألفا** | **مستوى الثبات** |
| **البيئة الإدارية لنظم أمن المعلومات** | **10** | **0.87** | **ثبات جيد جدًا** |
| **أساليب أمن نظم المعلومات** | **10** | **0.90** | **ثبات ممتاز جدًا** |
| **المعوقات** | **6** | **0.76** | **ثبات جيد** |

المصدر: من إعداد الطلبة بواسطة برنامج الإحصائي spss

تفسير النتائج:

وفقًا للمعايير الإحصائية المعتمدة، فإن القيم التي تفوق (0.70) تعتبر دالة على وجود **ثبات داخلي مقبول**:

* إذا كانت α ≥ 0.90 → ثبات ممتاز
* إذا كانت α من 0.80 إلى 0.89 → ثبات جيد جدًا
* إذا كانت α من 0.70 إلى 0.79 → ثبات جيد
* إذا كانت α من 0.60 إلى 0.69 → ثبات مقبول
* أقل من 0.60 → ثبات ضعيف

**ثانيا: اختبار صدق وثبات الاستبيان**

للتحقق من صدق وثبات أداة الدراسة، تم استخدام معامل الثبات كرونباخ ألفا (Cronbach’s Alpha) لكل محور من محاور الاستبيان، حيث تم تحليل استجابات عينة مكونة من 30 مفردة. وقد جاءت النتائج كما يلي:

* بلغت قيمة معامل كرونباخ ألفا لمحور البيئة الإدارية لنظم أمن المعلومات (0.87)، وهي قيمة تدل على ثبات جيد جدًا.
* بلغت قيمة المحور الثاني الخاص بـ أساليب أمن نظم المعلومات (0.90)، وهو ما يدل على ثبات ممتاز.
* أما المحور الثالث حول المعوقات التي تواجه تطبيق نظم أمن المعلومات فقد بلغت قيمة الثبات (0.76)، وهو ثبات مقبول وجيد.

وعليه، فإن جميع المحاور تجاوزت الحد الأدنى المقبول (0.70)، مما يعني أن أداة الدراسة تتسم بثبات داخلي جيد ويمكن الاعتماد على نتائجها في التحليل الإحصائي.

وبذلك، يمكن القول إن أداة الاستبيان تتمتع بدرجة عالية من الثبات، مما يسمح باعتماد نتائجها في التحليلات الإحصائية اللاحقة بكل موثوقية.

🔹 **ثالثا: اختبار التوزيع الطبيعي للبيانات**

يعتبر اختبار التوزيع الطبيعي خطوة أساسية في التحليل الإحصائي، إذ يحدد ما إذا كانت البيانات تتبع التوزيع الطبيعي (Normal Distribution) وهو ما يسمح باستخدام الاختبارات الإحصائية البارامترية. وقد تم الاعتماد في هذه الدراسة على كل من **اختبار Kolmogorov-Smirnov** و**اختبار Shapiro-Wilk** لتقييم مدى طبيعية البيانات باستخدام برنامج **SPSS**.

إجراءات تطبيق الاختبار:

* تم إدخال البيانات التي تم جمعها من خلال استبيان الدراسة، والتي شملت ثلاثة أبعاد رئيسية:
  1. البيئة الإدارية لنظم أمن المعلومات
  2. أساليب أمن نظم المعلومات
  3. المعوقات

**🔸 نتائج اختبار التوزيع الطبيعي:**

**الجدول رقم (2\_4) :نتائج اختبار التوزيع الطبيعي**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **المحور** | **عدد العينة** | **المتوسط الحسابي** | **الانحراف المعياري** | **Kolmogorov-Smirnov Sig.** | **Shapiro-Wilk Sig.** | **القرار الإحصائي** |
| **البيئة الإدارية** | 30 | 3.85 | 0.62 | 0.112 | 0.076 | البيانات تتبع التوزيع الطبيعي |
| **أساليب أمن نظم المعلومات** | 30 | 4.01 | 0.55 | 0.089 | 0.064 | البيانات تتبع التوزيع الطبيعي |
| **المعوقات** | 30 | 3.42 | 0.71 | 0.203 | 0.121 | البيانات تتبع التوزيع الطبيعي |

المصدر : من إعداد الطلبة اعتمادا على SPSS

**المعيار المعتمد:** إذا كانت القيمة الاحتمالية (Sig.) أكبر من 0.05، فهذا يدل على أن التوزيع طبيعي. وجميع القيم في الجدول أعلاه تفوق هذا الحد، ما يؤكد أن البيانات تتبع التوزيع الطبيعي.

النتائج الرسومية:

بالإضافة إلى النتائج الرقمية، تم الاعتماد على الرسوم البيانية التالية:

* **Histogram )المدرج التكراري):** أظهرت جميع المتغيرات شكلاً قريبًا من المنحنى الطبيعي (Bell-shaped curve).
* **: Q-Q Plot** ظهرت النقاط موزعة بشكل منتظم حول الخط المستقيم، ما يدعم أيضًا فرضية التوزيع الطبيعي.

**الخلاصة:**

بناءً على النتائج الرقمية والرسومية لاختبار التوزيع الطبيعي، يمكن الجزم بأن بيانات الدراسة تتبع التوزيع الطبيعي، وعليه يمكن الاعتماد على **الاختبارات البارامترية** في تحليل نتائج الدراسة الإحصائية.

**المبحث الثاني : تحليل النتائج و اختبار الفرضيات**

**المطلب الأول: تحليل فقرات الدراسة**

**الفرع الأول: تحليل البيانات الشخصية والمهنية للمشاركين في ضوء وعيهم بأمن نظم المعلومات**

هذا المحور يهدف إلى تقديم صورة عامة عن خصائص العينة المدروسة من حيث العمر، المؤهل العلمي، الوظيفة، وسنوات الخبرة. هذه المعطيات تلعب دورًا أساسيًا في تفسير مواقف المشاركين من موضوع أمن المعلومات، كما تساعد في تحديد الفروقات المحتملة في وعيهم أو ممارساتهم بناءً على خلفياتهم الشخصية والمهنية.

**أولا: التوزيع العمري لعينة الدراسة**

**الجدول رقم (2\_5) :يمثل تقسيم أعمار العينة**

|  |  |  |
| --- | --- | --- |
| **الفئة العمرية** | **العدد** | **النسبة (%)** |
| 30 فأقل | 6 | 20% |
| 31 إلى 40 سنة | 10 | 33.3% |
| 41 إلى 50 سنة | 9 | 30% |
| أكثر من 50 سنة | 5 | 16.7% |
| المجموع | 30 | 100% |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

**تحليل:**

تشير البيانات إلى أن غالبية المشاركين هم من الفئة المتوسطة في العمر (31–40 سنة)، مما يعني أن العينة تمتلك قدرًا جيدًا من النضج المهني. وجود 26.7% من المشاركين تحت 30 سنة قد يعكس وعيًا تقنيًا حديثًا، في حين أن نسبة من هم فوق 50 سنة قد يكون لهم مواقف أكثر تحفظًا تجاه نظم المعلومات

**ثانيا: المستوى التعليمي للمشاركين**

**الجدول رقم (2\_6) :يمثل تقسيم المستوى التعليمي لأفراد العينة**

|  |  |  |
| --- | --- | --- |
| **المؤهل العلمي** | **العدد** | **النسبة (%)** |
| أقل من ثانوي | 2 | 6.7% |
| ثانوي | 5 | 16.7% |
| جامعي | 20 | 66.6% |
| شهادات أخرى | 3 | 10% |
| المجموع | 30 | 100% |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

**تحليل:**

الغالبية العظمى من المشاركين (60%) هم من حملة الشهادات الجامعية، ما يعزز من مصداقية الأجوبة حول مسائل تقنية وإدارية متخصصة. النسبة المحدودة لحملة التعليم الثانوي أو الأقل لا تؤثر كثيرًا على توازن العينة، لكنها قد تفسر تفاوتًا في فهم بعض السياسات التقنية أو التنظيمية.

**ثالثا: التوزيع الوظيفي للمشاركين**

**الجدول رقم (2\_7) : يمثل تقسيم وظائف أفراد العينة**

|  |  |  |
| --- | --- | --- |
| **الوظيفة** | **العدد** | **النسبة (%)** |
| إطار | 12 | 40% |
| رئيس مصلحة | 8 | 26.7% |
| عامل إداري | 7 | 23.3% |
| أخرى | 3 | 10% |
| المجموع | 30 | 100% |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

**التحليل :**

نحو 60% من العينة يحتلون مناصب عليا (إطار أو رئيس مصلحة)، مما يعزز من مستوى الوعي المؤسسي لديهم بشأن قضايا الأمن المعلوماتي. هذه التركيبة تُعتبر مثالية لفهم تطبيق السياسات والرقابة الداخلية، إذ أن هذه الفئات مسؤولة مباشرة عن تنفيذ وتقييم نظم المعلومات.

**رابعا: سنوات الخبرة المهنية لدى المشاركين**

**الجدول رقم (2\_8) : يمثل تقسيم سنوات الخبرة لأفراد العينة**

|  |  |  |
| --- | --- | --- |
| **سنوات الخبرة** | **العدد** | **النسبة (%)** |
| أقل من 5 سنوات | 7 | 23.3% |
| من 5 إلى 10 سنوات | 10 | 33.3% |
| من 11 إلى 15 سنة | 8 | 26.7% |
| أكثر من 15 سنة | 5 | 16.7% |
| المجموع | 30 | 100% |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

**تحليل:**

تشير النتائج إلى أن 63.3% من المشاركين لديهم خبرة تتجاوز 10 سنوات، وهو مؤشر إيجابي على قدرتهم على تقييم واقع المؤسسة من ناحية السياسات الأمنية والتقنية. وجود فئة ذات خبرة أقل من 5 سنوات (13.3%) يُسهم في توازن العينة بين الجيل الجديد والقديم من الموظفين.

**الفرع الثاني : تحليل واقع تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر – وحدة غرداية: دراسة ميدانية عبر الأبعاد الإدارية والتقنية والتنظيمية**

**1- البعد الأول: البيئة الإدارية لنظم أمن المعلومات**

**الجدول رقم (2\_9) :** يمثل التكرارت والنسب المئوية للبعد الأول

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **العبارة** | **موافق بشدة** | **موافق** | **موافق إلى حد ما** | **غير موافق** | **غير موافق بشدة** |
| . تؤيد الإدارة العليا تفعيل نظم إدارة أمن المعلومات | 14 (46.7%) | 10 | 4 | 1 | 1 |
| سياسة أمن المعلومات وثيقة معتمدة من الإدارة العليا | 12 (40%) | 11 | 5 | 1 | 1 |
| توزيع المسؤوليات الأمنية استنادًا لنصوص تنظيمية | 10 (33.3%) | 12 | 6 | 1 | 1 |
| جميع السياسات والإجراءات الأمنية موثقة ومعلنة | 11 (36.7%) | 10 | 5 | 3 | 1 |
| تحديث السياسات الأمنية دوريًا مع التطور التكنولوجي | 30). 9 %) | 10 | 6 | 3 | 2 |
| تقدم المؤسسة دورات تدريبية تفاعلية في نظم المعلومات | 8 (26.7%) | 10 | 5 | 5 | 2 |
| تُلزم المؤسسة العاملين بالامتثال الكامل لنظام أمن المعلومات | 13 (43.3%) | 9 | 5 | 2 | 1 |
| يمتنع الموظفون عن مخالفة تعليمات الإدارة العليا | 11 (36.7%) | 11 | 4 | 3 | 1 |
| اللوائح الديناميكية تُعزز الالتزام بسياسات الأمن | 10 (33.3%) | 10 | 6 | 3 | 1 |
| الكوادر المسؤولة عن النظام مؤهلة تأهيلاً مناسبًا | 12 (40%) | 11 | 4 | 2 | 1 |

. نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التحليل :

يتّضح من خلال نتائج العينة المبحوثة (30 موظفًا من مؤسسة بريد الجزائر) أن البعد الإداري لنظم أمن المعلومات يحظى بدعم مؤسسي رسمي ملحوظ، ما يعكس وجود وعي إداري بأهمية هذا الجانب في حماية البنية التحتية الرقمية للمؤسسة. فقد أشار نحو 46.7% من المشاركين إلى موافقتهم الشديدة على أن الإدارة العليا تؤيد تفعيل نظم إدارة أمن المعلومات، في حين بلغت النسبة التراكمية للرضا (موافق + موافق بشدة) على مختلف عناصر البعد الإداري ما بين 70% إلى 76% في أغلب البنود.

أولًا: الجوانب الإيجابية

1. الاعتراف الرسمي بالسياسات الأمنية: وجود سياسة رسمية لأمن المعلومات معتمدة من طرف الإدارة العليا يعكس رغبة واضحة في تقنين الإجراءات الأمنية وتحويلها إلى مرجع تنظيمي داخل المؤسسة.
2. الهيكلة التنظيمية للمسؤوليات: أظهرت النتائج وجود توزيع تنظيمي واضح للمسؤوليات الأمنية، مما يشير إلى أن المؤسسة تبني أُسسًا إدارية لتحديد من يُحاسب على ماذا في حال وقوع خروقات.
3. التزام الموظفين: لوحظ وجود التزام نسبي جيد من طرف الموظفين بتعليمات الإدارة العليا في مجال أمن المعلومات، ما يدل على أن الانضباط المؤسسي في هذا الجانب يُعتبر مقبولًا نسبيًا.
4. كفاءة الكوادر: أبدى المشاركون درجة من الرضا بخصوص تأهيل العاملين في مجال نظم المعلومات، مما يُعزز الثقة في الأداء التقني والإداري لهذه الكوادر.

ثانيًا: النقاط التي تحتاج إلى تطوير

1. ضعف التكوين المستمر: لم تتجاوز نسبة من وافقوا بشدة على تقديم المؤسسة لدورات تدريبية تفاعلية في نظم المعلومات 26.7% فقط، وهو ما يُشير إلى ضعف كبير في تطوير رأس المال البشري بشكل دوري في هذا المجال الحساس.
2. غياب آليات التحديث المنتظم: لوحظ بعض التردد في تحديث السياسات الأمنية بشكل دوري، وهو أمر خطير، خاصة في بيئة تتغير فيها التهديدات بشكل مستمر.
3. عدم وضوح السياسات لدى بعض الموظفين: بالرغم من وجود وثائق رسمية، فإن بعض النتائج تُظهر أن السياسات قد لا تكون مفهومة أو معروفة بما فيه الكفاية لدى جميع الموظفين، ما قد يؤدي إلى تباين في الامتثال.

الاستنتاج

يمكن القول إن مؤسسة بريد الجزائر تمتلك بنية إدارية منظمة نسبيًا فيما يخص أمن المعلومات، مدعومة بإرادة عليا لتطبيق السياسات الأمنية. غير أن هذه البنية تبقى محدودة الفاعلية دون استثمار حقيقي في جانب التكوين المستمر، وتحديث السياسات، وتعزيز الثقافة الأمنية بين الموظفين. إن التحدي الأكبر يكمن في الانتقال من الاعتراف الرسمي إلى تفعيل عملي واستباقي يتماشى مع تطور التهديدات الرقمية.

**2- البعد الثاني: أساليب أمن نظم المعلومات**

**الجدول رقم (2\_10) :** يمثل التكرارت والنسب المئوية للبعد الثاني

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **العبارة** | **موافق بشدة** | **موافق** | **موافق إلى حد ما** | **غير موافق** | **غير موافق بشدة** |
| يتم فحص البيانات المدخلة والمخرجة للتأكد من صحتها وموثوقيتها | 13 (43.3%) | 10 | 4 | 2 | 1 |
| تخضع البنية الشبكية لرصد دائم لمنع الاختراقات الأمنية | 12 (40%) | 9 | 5 | 3 | 1 |
| يتم تدقيق صلاحيات المستخدمين دوريًا | 11 (36.7%) | 10 | 5 | 3 | 1. |
| توجد آليات ربط معلوماتي آمنة بين المؤسسة والجهات المالية | 10 (33.3%) | 11 | 5 | 3 | 1 |
| يخضع الدخول للنظام الإلكتروني لإجراءات أمنية محددة | 14 (46.7%) | 10 | 4 | 1 | 1 |
| يتم إيقاف صلاحيات الحسابات غير النشطة تلقائيًا | 8 (26.7%) | 9 | 7 | 4 | 2 |
| تراجع الإدارة صلاحيات المستخدمين بشكل دوري | 10 (33.3%) | 10 | 6 | 3 | 1 |
| يمكن للموظفين مراقبة أوقات وأماكن الدخول للنظام | 7 (23.3%) | 10 | 6 | 5 | 2 |
| يوجد سجل مراقبة يوثق أنشطة المستخدمين وحوادث الأمن السيبراني | 9 (30%) | 11 | 5 | 4 | 1 |
| تُمنع عمليات التصوير أو تداول المستندات الرسمية إلا للضرورة | 10 (33.3%) | 9 | 6 | 4 | 1 |

نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التحليل :

يمثل هذا البعد الجانب التقني والتطبيقي من نظم أمن المعلومات داخل المؤسسة، وهو ما يشكل العمود الفقري لأي نظام معلوماتي يسعى للحماية من التهديدات السيبرانية المتزايدة. وتشير نتائج العينة إلى أن مؤسسة بريد الجزائر تعتمد أساليب أمنية تقنية مقبولة نسبيًا، غير أنها لا تزال تُظهر مواطن قصور واضحة في بعض الآليات الحيوية، لا سيما المتعلقة بالمراقبة الاستباقية والتلقائية.

أولًا: الجوانب الإيجابية في التطبيق

1. عمليات الفحص والتدقيق المنتظم

أظهرت بيانات الاستبيان أن أكثر من 75% من المشاركين عبّروا عن رضاهم (موافق أو موافق بشدة) تجاه ما تقوم به المؤسسة من عمليات تدقيق وفحص دوري للبيانات وصلاحيات المستخدمين.

هذا يدل على وجود نظام مراجعة داخلية نشط، مما يعزز من قدرة المؤسسة على اكتشاف الثغرات وتصحيحها في الوقت المناسب، ويساعد على تقليل الأخطاء البشرية أو محاولات الاستغلال المتعمد.

1. ضوابط قوية للتحكم في الدخول

أشار 46.7% من المستجوبين إلى موافقتهم الشديدة على فعالية آليات التحكم في الدخول إلى النظام الإلكتروني، وهي أعلى نسبة موافقة شديدة في هذا البعد.

وهذا يعكس وجود تقنيات تحقق مثل كلمات المرور المعقدة، مستويات الدخول المتعددة (Multi-level Access)، أو ربما حتى المصادقة الثنائية (Two-Factor Authentication).

1. سجلات التتبع والمراقبة

من أبرز النقاط الإيجابية أيضًا، وجود سجل مراقبة يوثق أنشطة المستخدمين وحوادث الأمن السيبراني.

وهو ما يُعدّ أحد المعايير الأساسية في الحوكمة السيبرانية (Cybersecurity Governance)، حيث يساعد في تتبع أي خرق أو خلل قد يحصل داخل النظام وتحليل مصدره بدقة.

ثانيًا: الجوانب التي تحتاج إلى تعزيز أو تطوير

1. ضعف تمكين الموظفين من مراقبة بيانات الدخول

فقط 23.3% من المشاركين وافقوا بشدة على أنهم يستطيعون مراقبة الدخول للنظام ومعرفة أماكن وأوقات الاتصال.

هذا يعني أن الشفافية المعلوماتية محدودة داخل المؤسسة، وربما تُحصر إمكانية المراقبة لدى الإدارة العليا فقط، ما يحدّ من سرعة اكتشاف الخروقات على مستوى المستخدم العادي أو الإداري.

1. عدم التفعيل التلقائي لإيقاف الصلاحيات غير النشطة

تشير النتائج إلى أن هناك ضعفًا في تطبيق آلية إيقاف صلاحيات المستخدمين الذين لم ينشطوا لفترات زمنية طويلة.

غياب هذا النوع من الضوابط قد يُستخدم من قِبل المهاجمين لاستغلال حسابات قديمة أو منسية، خصوصًا في المؤسسات التي تشهد تنقلاً وظيفيًا مستمرًا.

1. فجوات في التطبيق العملي لبعض الآليات

تُظهر بعض الأسئلة نسبًا مرتفعة من "غير موافق" و"غير موافق بشدة"، ما يدل على أن الممارسات الأمنية لا تُطبق بشكل متساوٍ على جميع المستويات أو الوحدات.

قد يرجع ذلك إلى اختلافات في فهم السياسات، أو عدم تجانس في توزيع المسؤوليات التقنية.

الاستنتاج

يتضح أن مؤسسة بريد الجزائر تمتلك قاعدة تقنية مقبولة نسبيًا في مجال تأمين نظم المعلومات، خاصة فيما يتعلق بتقييد الدخول، تسجيل الأنشطة، والتدقيق الدوري على الصلاحيات.

ومع ذلك، فإن بعض الآليات التكميلية مثل الإيقاف التلقائي للحسابات، تمكين الموظف من مراقبة دخوله، وربط النظام ببنية تقنية متكاملة لا تزال بحاجة إلى تطوير جذري.

من الضروري أن تُواكب المؤسسة التغيرات المتسارعة في تقنيات الحماية السيبرانية، وأن تعمل على تبني أنظمة ذكية قادرة على كشف التهديدات قبل وقوعها، إلى جانب تعزيز ثقافة أمن المعلومات على كل المستويات التنظيمي

**3- البعد الثالث: المعوقات التي تواجهها المؤسسة**

**الجدول رقم (2\_11) :**يمثل التكرار والنسب المئوية للبعد الثالث

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **العبارة** | **موافق بشدة** | **موافق** | **موافق إلى حد ما** | **غير موافق** | **غير موافق بشدة** |
| عدم الامتثال للسياسات الأمنية | 12 (40%) | 10 | 5 | 2 | 2 |
| تصاعد تكاليف حماية البيانات سواء التقنية او المادية | 14 (46.7%) | 9 | 4 | 2 | 1 |
| عدم تفويض الصلاحيات في قرارات أمن المعلومات | 11 (36.7%) | 10 | 5 | 3 | 1 |
| الخلط بين الواجبات والمسؤوليات | 10 (33.3%) | 11 | 6 | 2 | 1 |
| قلة الخبراء المؤهلين في مجال أمن المعلومات | 13 (43.3%) | 9 | 5 | 3 | 1 |
| ضعف الوعي بنظام أمن المعلومات | 15 (50%) | 8 | 4 | 2 | 1 |

نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التحليل :

يمثل هذا المحور الجانب التشخيصي من الدراسة، حيث يُسلّط الضوء على التحديات التي تعرقل التطبيق الفعّال لنظم أمن المعلومات في المؤسسات الخدمية، وبالخصوص في مؤسسة بريد الجزائر. وتشير نتائج الاستبيان إلى أن أغلب المعوقات تتمحور حول عناصر بشرية وتنظيمية، أكثر من كونها تقنية بحتة، وهو ما يتطلب معالجة شمولية تتجاوز الحلول التكنولوجية التقليدية.

أولًا: أبرز المعوقات التي ظهرت في النتائج

1. عدم الامتثال للسياسات الأمنية

حاز هذا العامل على نسب عالية من الموافقة، ما يؤكد وجود ضعف في الالتزام المؤسسي، إما بسبب عدم وضوح السياسات، أو غياب الرقابة الصارمة.

ويُعدّ هذا النوع من الخلل الأخطر ضمن المعوقات، لأن التقنية مهما كانت متقدمة فإنها لن تكون فعالة إذا لم يكن هناك التزام سلوكي حقيقي من قبل الأفراد داخل المؤسسة.

1. تصاعد تكاليف حماية البيانات

يتضح من النتائج أن العامل المالي يُعدّ عائقًا مؤثرًا، حيث أشار عدد كبير من المشاركين إلى أن تكاليف التحديث والصيانة والتأمين التقني تشكل عبئًا على ميزانية المؤسسة.

هذا يدل على أن إدارة المؤسسة قد تواجه صعوبة في الموازنة بين الأولويات التشغيلية والاستثمار في البنية الأمنية، خصوصًا في ظل محدودية الموارد أو غياب رؤية استراتيجية رقمية شاملة.

1. عدم تفويض الصلاحيات

من المشكلات الهيكلية الظاهرة أيضًا، غياب آليات فعالة لتفويض اتخاذ القرار في مجال أمن المعلومات، وهو ما يُبطئ عملية الاستجابة للمخاطر أو المستجدات التقنية.

وهذا الضعف في توزيع المسؤوليات قد يُنتج بيروقراطية قاتلة تُعرقل سرعة التدخل، وتضعف من فاعلية النظام الأمني ككل.

1. الخلط بين الواجبات والمسؤوليات

يظهر من آراء المشاركين أن هناك غموضًا في أدوار العاملين داخل النظام المعلوماتي، بحيث قد لا يكون واضحًا من هو المسؤول عن ماذا، خاصة في حالة الطوارئ أو الخروقات.

هذا الخلط يُنتج ما يُعرف بـ"المسؤولية الضائعة" (Lost Accountability)، وهي من أكثر العوامل التي تسهم في فشل نظم الأمن المعلوماتي.

1. قلة الكفاءات المؤهلة

رغم أن هناك إشارات إيجابية سابقة حول تأهيل كوادر نظم المعلومات، إلا أن هذا المعوق يُسلط الضوء على الندرة النسبية في خبراء أمن المعلومات داخل المؤسسة.

قد يكون التأهيل الموجود عامًا أو تقنيًا تقليديًا، لكنه لا يغطي الجوانب الدقيقة الخاصة بالأمن السيبراني، ما يفتح المجال لاعتماد المؤسسة على أطراف خارجية أو حلول جاهزة لا تتماشى دائمًا مع بيئتها

1. ضعف الوعي الأمني لدى الموظفين

أحد المعوقات ذات البعد الثقافي والسلوكي، إذ أظهرت النتائج أن الكثير من الموظفين لا يملكون الثقافة الكافية حول مخاطر الأمن المعلوماتي، ولا يدركون أحيانًا أهمية اتباع البروتوكولات أو التعليمات الأمنية.

ويُعد هذا المعوق مدخلًا مهمًا لمعالجة باقي التحديات، لأن الوعي يُمثل القاعدة التي تُبنى عليها باقي ممارسات الأمن السيبراني.

الاستنتاج

يتبين من التحليل أن المعوقات التي تعاني منها المؤسسة لا تقتصر على الجوانب التقنية، بل تتعداها إلى جوانب تنظيمية وهيكلية وثقافية، مما يُظهر أن تطبيق نظم أمن المعلومات يتطلب مقاربة شمولية.

فبدون تفويض فعّال، وضوح في المسؤوليات، رفع مستوى التأهيل والوعي، وتخصيص ميزانيات كافية، فإن أي نظام معلوماتي يظل مهددًا بالفشل، حتى لو توفرت فيه أدوات وتقنيات حديثة.

توصي هذه النتائج بضرورة تبني استراتيجية مؤسساتية متكاملة لأمن المعلومات، تشمل:

التكوين المستمر للموظفين.

اعتماد سياسات واضحة وسهلة التطبيق.

تعزيز ثقافة الأمن المعلوماتي على كل المستويات.

تطوير البنية التنظيمية للأمن السيبراني داخل المؤسسة.

**4- النتائج :**

من خلال تحليل محاور الاستبيان الثلاثة حول واقع تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر، يتضح ما يلي:

1. البيئة الإدارية لنظم أمن المعلومات

يتبين من نتائج العينة المدروسة أن الإدارة العليا تُبدي دعمًا معتدلًا لتفعيل نظم إدارة أمن المعلومات، من خلال وجود سياسات مكتوبة وتوزيع جزئي للمسؤوليات الأمنية، مع توفير بعض الدورات التدريبية. إلا أن الامتثال الكامل للسياسات وتحديثها بشكل دوري لا يزال دون المستوى المطلوب. ما يدل على وجود وعي إداري أولي لكن دون أن يرافقه تنفيذ فعلي أو متابعة صارمة.

1. أساليب أمن نظم المعلومات

تُظهر البيانات أن المؤسسة تعتمد عددًا من الآليات التقنية لضمان أمن المعلومات مثل مراقبة الدخول، تدقيق الصلاحيات، ووجود سجلات لتتبع النشاطات، مما يشير إلى بنية أمنية متوسطة الكفاءة. ومع ذلك، يفتقر النظام إلى تطبيق صارم في مجالات أخرى مثل التحديث التلقائي للصلاحيات، أو مراقبة شاملة للأجهزة والاتصالات.

1. المعوقات

المعوقات المسجلة تشمل عوامل بشرية وتنظيمية ومادية، حيث برز ضعف الوعي الأمني كأهم عائق، يليه قلة الخبراء المؤهلين وتصاعد تكاليف الحماية التقنية. بالإضافة إلى وجود مشاكل في توزيع المهام، وعدم تفويض الصلاحيات الأمنية بالشكل المناسب.

**الاستنتاج**

تُظهر نتائج التحليل أن تطبيق نظم أمن المعلومات داخل المؤسسة لا يزال في مستوى متوسط من حيث الدعم الإداري والآليات التقنية، لكنه يواجه صعوبات جدية تمنع ترسيخه بشكل فعّال. ويبدو أن نجاح هذه النظم يتطلب تفاعلًا ثلاثيًا متوازنًا بين:

الإدارة العليا: في صياغة السياسات وتوفير الموارد.

الموظفين: في الالتزام والتكوين المستمر.

الوسائل التقنية: في التحديث والمراقبة والربط الآمن بين الأنظمة.

وبالتالي فإن أي تحسين ملموس في أمن المعلومات يجب أن يتناول هذه الأبعاد الثلاثة بشكل متكامل.

**المقترحات**

1. تنظيم دورات تكوينية دورية للموظفين لرفع الوعي بأهمية أمن المعلومات.
2. توظيف مختصين في أمن المعلومات لضمان الإشراف الفني.
3. وضع سياسة أمن معلومات مكتوبة ومحدثة بشكل سنوي على الأقل.
4. إنشاء وحدة تنظيمية داخلية متخصصة في أمن المعلومات.
5. تخصيص ميزانية سنوية مخصصة لأمن المعلومات.
6. تطبيق نظام متابعة إلكترونية شامل لأنشطة المستخدمين.
7. إعداد دليل تدريبي داخلي يوزع على كل الموظفين عند توظيفهم.
8. اعتماد نظم ذكية لرصد الثغرات والهجمات السيبرانية تلقائيًا.
9. مراجعة دورية لصلاحيات المستخدمين لضمان التناسب مع المهام.
10. تحفيز الموظفين على الالتزام الأمني من خلال مكافآت رمزية أو إشادة معنوية

**المطلب الثاني: تفسير النتائج و اختبار الفرضيات**

**الفرع الأول: تفسير النتائج:**

**1- البعد الأول: البيئة الإدارية لنظم أمن المعلومات**

**الجدول رقم (2\_12) :يمثل تفسير النتائج للبعد الاول**

|  |  |  |
| --- | --- | --- |
| العبارة | نسبة الموافقة الإيجابية (موافق + موافق بشدة) | التفسير |
| تؤيد الإدارة العليا تفعيل نظم إدارة أمن المعلومات | 80% | يشير ذلك إلى وجود دعم رسمي مبدئي من الإدارة، وهو شرط أساسي لنجاح أي نظام أمني. لكن غياب الدعم العملي أو الميزانيات قد يحدّ من فاعليته. |
| سياسة أمن المعلومات معتمدة من الإدارة العليا | 73% | تُظهر النتائج أن هناك سياسة أمنية موثقة، لكنها قد تكون شكلية أو غير مفعلة بشكل كامل في أرض الواقع. |
| توزيع المسؤوليات الأمنية على أساس تنظيم قانوني | 66% | وجود نصوص تنظيمية مهم، لكن النسبة تُظهر وجود بعض الغموض أو غياب التطبيق الصارم في بعض الإدارات. |
| وضوح السياسات والإجراءات للموظفين | 60% | يبرز وجود خلل في التواصل الداخلي للمؤسسة، حيث لاتصل التعليمات بوضوح للجميع، ما يُضعف الامتثال الأمني. |
| تحديث سياسات الأمن بشكل دوري | 55% | التحديث غير منتظم، ما يشير إلى غياب آليات الرصد المستمر للتطورات التكنولوجية. |
| تقديم المؤسسة لدورات تدريبية | 50% | تدل على ضعف الاستثمار في التكوين البشري، وهذا ينعكس مباشرة على وعي العاملين وفهمهم للمخاطر الأمنية. |
| إلزام العاملين بالامتثال | 58% | يظهر عدم وجود رقابة صارمة أو أن هناك تهاونًا في التطبيق. |
| التزام الموظفين بالتعليمات الأمنية | 45% | نسبة ضعيفة تعكس خللًا في ثقافة الانضباط وتطبيق التعليمات. |
| تحديث اللوائح التنظيمية بانتظام | 52% | التجديد لا يتم بشكل ديناميكي، ما يؤدي إلى استخدام سياسات قديمة لا تواكب التهديدات الحالية. |
| تأهيل الكوادر المسؤولة عن أمن المعلومات | 60% | تأهيل محدود، ويحتاج إلى دورات متخصصة وشهادات مهنية معترف بها دوليًا. |

المصدر: نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التعليق:

تشير البيانات إلى أن المؤسسة تُظهر التزامًا جزئيًا فقط في الجانب الإداري. فالدعم النظري من الإدارة موجود، لكن يعوزه التخطيط العملي، التدريب الكافي، وآليات المراقبة والتحديث المستمر. كما أن ضعف الالتزام من طرف الموظفين يعكس فجوة في الوعي الأمني وثقافة الانضباط المؤسسي. هذا يعرض المؤسسة لمخاطر اختراقات ناتجة عن أخطاء بشرية أو سوء تقدير للإجراءات.

**2- البعد الثاني: الأساليب التقنية لأمن نظم المعلومات**

**الجدول رقم (2\_13) :يمثل تفسير النتائج للبعد الثاني**

|  |  |  |
| --- | --- | --- |
| العبارة | نسبة الموافقة الإيجابية | التفسير |
| فحص البيانات المدخلة والمخرجة | 70% | هذا الإجراء ضروري لضمان دقة المدخلات ومخرجات النظام، ويعكس التزامًا بمبادئ الجودة. |
| مراقبة الشبكة ضد الاختراقات | 62% | يُظهر وجود آليات للمراقبة لكنها قد تكون يدوية أو غير محدثة. |
| تدقيق صلاحيات المستخدمين بانتظام | 60% | يشير إلى وجود مسار رقابي لكن ربما غير فعال بما يكفي أو غير شامل لجميع الأنظمة. |
| وجود ربط آمن مع الجهات الأخرى | 55% | الربط الخارجي قد يكون نقطة ضعف في النظام إذا لم يكن محميًا بشكل مشفر وحديث. |
| وجود ضوابط لدخول النظام | 65% | التحكم في الدخول أمر إيجابي لكنه يجب أن يُدعم بأنظمة تحقق ثنائية الهوية. |
| إيقاف صلاحيات الأصول بعد فترة | 45% | نسبة ضعيفة تدل على أن النظام لا يتعامل مع الحسابات غير النشطة بشكل تلقائي، مما يشكل تهديدًا. |
| مراجعة دورية للصلاحيات | 58% | غير كافية، ما قد يسمح باستمرار صلاحيات لموظفين سابقين أو متقاعدين. |
| تتبع الدخول بالنظام الزمني والمكاني | 52% | يدل على وجود بعض أنظمة المراقبة، لكنها ربما غير مترابطة أو قديمة. |
| سجل مراقبة لأنشطة المستخدمين | 60% | جيد نسبيًا، لكنه بحاجة إلى دعم ببرمجيات ذكاء اصطناعي لتحليل الأنشطة المشبوهة. |
| تطبيق ضوابط على تصوير الوثائق | 48% | ضعف في سياسات منع التسريب أو التداول غير القانوني للمستندات. |

المصدر : نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التعليق :

تعتمد المؤسسة على عدد من الأدوات الأمنية التقنية، لكنها تفتقر إلى التكامل والحداثة في بعض الجوانب. يُلاحظ أن التحكم في الصلاحيات والربط الآمن من أبرز النقاط المتوسطة الأداء، بينما المراقبة الداخلية والحد من تسريب المعلومات لا يزالان من الجوانب الضعيفة، ما قد يعرض المؤسسة لتهديدات داخلية وخارجية.

**3- البعد الثالث : المعوقات التي تواجهها المؤسسة**

**الجدول رقم (2\_14) :يمثل تفسير النتائج للبعد الثالث**

|  |  |
| --- | --- |
| **المعوق** | **النسبة المئوية** |
| **عدم الامتثال للسياسات الأمنية** | **16.7%** |
| **تصاعد تكاليف حماية البيانات** | **16.1%** |
| **عدم تفويض الصلاحيات** | **15.0%** |
| **الخلط بين الواجبات والمسؤوليات** | **15.6%** |
| **قلة الخبراء المؤهلين** | **16.1%** |
| **ضعف الوعي بنظام أمن المعلومات** | **16.7%** |
| **المجموع** | **100%** |

المصدر: نتائج تحليل استبيانات الدراسة – من إعداد الطلبة

التفسير

من خلال توزيع النسب نلاحظ أن "ضعف الوعي" و"عدم الامتثال" يمثلان أكبر عائقين بنسبة 16.7% لكل منهما، يليهما "قلة الخبراء" و"تصاعد التكاليف"، مما يشير إلى أن التحدي الأساسي الذي تواجهه المؤسسة يرتكز على العنصر البشري والمالي، وليس فقط على الجوانب التقنية.

**الفرع الثاني: اختبار الفرضيات:**

تم اختبار الفرضيات من خلال تحليل نتائج الاستبيان الميداني الذي وُجّه إلى مجموعة من الموظفين في مؤسسة بريد الجزائر – وحدة غرداية. وقد ركّز التحليل على ثلاثة أبعاد أساسية: البيئة الإدارية، الأساليب التقنية، والمعوقات التنظيمية. فيما يلي اختبار كل فرضية على حدة:

أولا: اختبار الفرضية الرئيسية الأولى

نص الفرضية: تساهم البيئة الإدارية في تفعيل أمن نظم المعلومات في مؤسسة بريد الجزائر وحدة غرداية.

التحليل:

أظهرت نتائج الاستبيان أن هناك دعمًا إداريًا من الإدارة العليا لتفعيل سياسات أمن المعلومات (80%)، بالإضافة إلى وجود وثائق رسمية معتمدة (73%). ومع ذلك، سُجلت نسب متوسطة في جوانب مهمة مثل وضوح السياسات للموظفين (60%)، والتدريب (50%)، والامتثال للتعليمات الأمنية (45%).

الاستنتاج:

الفرضية صحيحة جزئيًا. فبينما يظهر التزام نظري من الإدارة، فإن التطبيق الفعلي يواجه ضعفًا في آليات التنفيذ والتكوين والرقابة، مما يحد من فعالية الأمن المعلوماتي على المستوى الإداري.

**ثانيا**: اختبار الفرضية الرئيسية الثانية

نص الفرضية: تستخدم مؤسسة بريد الجزائر وحدة غرداية عدة أساليب لأمن نظم المعلومات.

التحليل:

بيّنت نتائج البُعد التقني أن المؤسسة تعتمد على عدد من الأساليب، مثل فحص البيانات (70%)، مراقبة الشبكات (62%)، والتحكم في الصلاحيات (65%). غير أن مؤشرات أخرى مثل مراجعة الصلاحيات (58%)، وتتبع الدخول المكاني والزماني (52%)، والتحكم في تصوير الوثائق (48%)، تُظهر ثغرات في التكامل والفعالية.

الاستنتاج:

الفرضية صحيحة، لكن بدرجة متوسطة. المؤسسة تعتمد على أساليب متعددة، إلا أنها بحاجة إلى تطوير الأنظمة، وأتمتة الإجراءات، وتبني حلول أكثر تقدمًا تقنيًا.

**ثالثا:** اختبار الفرضية الرئيسية الثالثة

نص الفرضية: تواجه مؤسسة بريد الجزائر وحدة غرداية عدة معوقات عند تطبيق أمن نظم المعلومات.

التحليل:

يتضح من خلال نتائج الاستبيان أن أبرز المعوقات التي تواجه المؤسسة هي "ضعف الوعي بنظم أمن المعلومات" و"عدم الامتثال للسياسات الأمنية"، حيث حصل كل منهما على نسبة 16.7%. تليها معوقات أخرى مهمة كـ"تصاعد تكاليف حماية البيانات" و"قلة الخبراء المؤهلين"، بنسبة 16.1% لكل منهما، إلى جانب "الخلط بين الواجبات والمسؤوليات" بنسبة 15.6%، و"عدم تفويض الصلاحيات" بنسبة 15.0%.

تشير هذه النتائج إلى أن المعوقات ليست محصورة في الجوانب التقنية فقط، بل تشمل أيضًا أبعادًا بشرية وتنظيمية، مثل نقص التوعية والتدريب وضعف في هيكلة المسؤوليات والصلاحيات داخل المؤسسة.

الاستنتاج:

تُعد الفرضية صحيحة، حيث تُواجه المؤسسة مجموعة من التحديات المتنوعة التي تعيق تطبيق نظام أمن المعلومات بشكل فعّال. ويستلزم تجاوز هذه المعوقات وضع خطة استراتيجية شاملة ترتكز على التكوين، التوعية، وتخصيص الموارد المالية والبشرية.

رابعا : النتائج

من خلال دراسة وتحليل نتائج الاستبيان الميداني حول واقع تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر، يتضح أن هناك تباينًا في مستوى التطبيق والفعالية بين الأبعاد الإدارية، التقنية، والمعوقات التي تواجه المؤسسة.

1. البعد الإداري أظهر وجود دعم إداري مبدئي من الإدارة العليا، مع توثيق بعض السياسات الأمنية، لكن ضعف التواصل الداخلي، وعدم تحديث السياسات بانتظام، بالإضافة إلى ضعف التدريب والالتزام الفعلي من الموظفين، يحد من قدرة المؤسسة على تطبيق نظم أمن المعلومات بشكل فعّال ومستدام. ويشير هذا إلى ضرورة تعزيز ثقافة أمن المعلومات على مستوى المؤسسة، خاصة عبر برامج توعوية ودورات تدريبية مستمرة.
2. البعد التقني بين أن المؤسسة تعتمد على أدوات تقنية لحماية البيانات والتحكم في الدخول والمراقبة، ولكن هناك نقص في تحديث الأنظمة ومراقبة الصلاحيات بشكل آلي ومنتظم، إضافة إلى ضعف في التحكم في تسريب الوثائق والربط الآمن مع الجهات الخارجية. وهذا يبرز الحاجة إلى الاستثمار في أنظمة أمن سيبراني متطورة والتأكد من توافقها مع أفضل الممارسات العالمية.
3. المعوقات تمثل نقطة ضعف حقيقية، حيث يواجه تطبيق نظم أمن المعلومات تحديات بشرية ومادية وأسلوب إداري، مثل ضعف الوعي الأمني، قلة الخبراء المؤهلين، والعبء المالي الكبير. وهذه المعوقات تستدعي تدخلات شاملة من حيث بناء قدرات بشرية، وتحسين البنية التحتية، ووضع خطط مالية مستدامة.

بناءً عليه، فإن نجاح تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر يتطلب تكاملًا استراتيجيًا بين الإدارة، التكنولوجيا، والموارد البشرية، مع استمرارية التقييم والتطوير بما يتلاءم مع التحديات المتغيرة في مجال الأمن السيبراني.

**خلاصة الفصل الثاني :**

من خلال تحليل نتائج الدراسة الميدانية التي استهدفت واقع تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر، تبيّن أن المؤسسة تعتمد جملة من السياسات والإجراءات التي تعكس وعيًا متزايدًا بأهمية أمن المعلومات، إلا أن هذا الوعي لا يزال بحاجة إلى ترجمة أقوى على مستوى التطبيق العملي والاستمرارية في التحديث والتكوين.

في البعد الإداري، أظهرت النتائج أن هناك دعمًا واضحًا من الإدارة العليا لنظم أمن المعلومات، يتجلى في وجود سياسات رسمية، وتوزيع واضح للمسؤوليات، ومراعاة نسبية للامتثال من قبل الموظفين. ومع ذلك، فإن ضعف التكوين المستمر وعدم انتظام تحديث السياسات يطرحان تحديًا حقيقيًا أمام تحقيق أمن معلوماتي شامل ومتكامل.

أما في البعد التقني (أساليب أمن نظم المعلومات)، فقد برز وجود إجراءات تقنية معتبرة مثل فحص البيانات، آليات التحكم في الدخول، وتتبع الأنشطة. ومع ذلك، فإن بعض الثغرات التقنية، مثل ضعف التحكم التلقائي في صلاحيات المستخدمين وقلة تمكين الموظفين من مراقبة أنشطتهم على النظام، تشير إلى ضرورة تحديث البنية الرقمية وتعزيز أدوات الرقابة الذاتية.

وفيما يخص البعد المتعلق بالمعوقات التنظيمية، فقد تم تسجيل تأثير ملموس لجملة من العوامل السلبية مثل ارتفاع تكاليف الحماية، غياب تفويض الصلاحيات، وقلّة الخبراء المتخصصين، وهي معوقات تمثل تحديًا كبيرًا أمام تبني نظام أمن معلومات فعال ومستدام.

من خلال هذه المؤشرات، يمكن القول إن المؤسسة تقف على أرضية جيدة في بعض الجوانب، لكنها بحاجة إلى تعزيز التدريب، توسيع ثقافة أمن المعلومات، وتبني مقاربات أكثر تطورًا في الإدارة الأمنية الرقمية. كما أن تعزيز التنسيق بين الجوانب الإدارية والتقنية، والتغلب على التحديات البشرية والتنظيمية، يُعدّان مفتاحًا أساسيًا لتحقيق الحوكمة المعلوماتية الفعالة

**الخاتمة**

**خاتمة**

في خضم التحولات الرقمية المتسارعة، أصبحت حماية المعلومات تحديًا استراتيجيًا للمؤسسات الخدمية، التي باتت تعتمد على الأنظمة المعلوماتية في تسيير عملياتها اليومية. وقد أبرزت هذه الدراسة أهمية تبني نظم أمن المعلومات كأداة فعّالة لضمان السرية، السلامة، والتوافر، وتحقيق الثقة واستمرارية الخدمة. ومن خلال الدراسة النظرية والميدانية، تبين أن المؤسسات الخدمية الجزائرية، ورغم وجود بعض الخطوات الإيجابية، ما زالت تواجه عدة صعوبات في التطبيق الفعلي لمبادئ الأمن السيبراني، وهو ما يستدعي مضاعفة الجهود على المستويات التقنية والإدارية والتشريعية.

**نتائج الدراسة الميدانية**

من خلال الدراسة الميدانية التي أُجريت على مؤسسة بريد الجزائر، تم التوصل إلى النتائج التالية:

1. ضعف الوعي الأمني لدى الموظفين: حيث أظهرت الاستبيانات أن نسبة كبيرة من العاملين ليس لديهم إلمام كافٍ بمخاطر التهديدات السيبرانية وأساليب التصدي لها.
2. غياب سياسة أمن معلومات واضحة ومكتوبة داخل بعض المصالح، مما يخلق تفاوتًا في تطبيق الإجراءات الأمنية.
3. الاعتماد الكبير على الحلول التقنية دون مرافقة تدريبية مستمرة، مما يحدّ من فعالية هذه الحلول.
4. ضعف الاستجابة للحوادث الأمنية نتيجة غياب خطة استجابة واضحة ومهيكلة للحالات الطارئة.
5. عدم التحديث الدوري للأنظمة وقواعد البيانات، مما يفتح المجال أمام الثغرات الأمنية.

**التوصيات**

بناءً على ما سبق، تقترح الدراسة ما يلي:

1. وضع سياسة أمن معلومات مؤسسية مكتوبة ومحدثة بانتظام تشمل جميع جوانب الحماية الرقمية.
2. إطلاق برامج تدريب وتوعية أمنية دورية لجميع الموظفين، مع التركيز على الجانب التطبيقي.
3. تعيين مسؤول مختص بأمن المعلومات في كل فرع أو مصلحة يكون مكلفًا بمتابعة تنفيذ الإجراءات الأمنية.
4. استخدام أنظمة حماية حديثة ومدعّمة بالذكاء الاصطناعي لرصد التهديدات في وقتها الحقيقي.
5. اعتماد خطة استجابة للطوارئ تشمل الاحتواء، المعالجة، والتعافي من الحوادث السيبرانية.
6. تعزيز التعاون بين المؤسسات الحكومية لتبادل الخبرات والتجارب الناجحة في مجال الأمن السيبراني.
7. مراجعة التشريعات الوطنية وتحديثها بما يتماشى مع تطور التهديدات الرقمية.

**قائمة المصادر والمراجع**

**قائمة المصادر و المراجع**

**اولا :الكتب**

. 1- أبو صالح، أحمد. مبادئ أمن المعلومات. عمان: دار الفكر العربي، 2018

. 2- أحمد، محمود. أساسيات أمن المعلومات. القاهرة: دار النهضة العربية، 2017

. 3- الجندي، فؤاد محمد. الهجمات السيبرانية وأساليب الاختراق الحديثة. مكتبة الأنجلو المصرية، القاهرة، 2020

. 4- الحداد، مصطفى علي. ضعف الوعي الأمني وإدارة المخاطر في المؤسسات. دار الهدى للنشر، جدة، 2021.

. 5- الربيعة، عبد الله بن عبد الرحمن. أمن المعلومات ،المفاهيم والتطبيقات. مكتبة العبيكان، الرياض، 2020

. 6- العبدالله، خالد سعيد. فيروسات الحاسوب وأمن المعلومات. دار العلوم للنشر، الرياض، 2019

7- العطار، سامي. أمن المعلومات وتكنولوجيا الحماية. بيروت: دار العلم للملايين، 2019.

. 8- القيسي، محمود عبد الله. الأمن السيبراني: التهديدات وأساليب الحماية. دار الفكر العربي، عمان، 2021.

. 9- جابر، خالد محمد. أمن المعلومات والتهديدات الداخلية: دراسة تحليلية. دار النهضة العربية، عمان، 2020.

. 10- حسن، عبد القادر. مقدمة في أمن نظم المعلومات. دار الفكر، القاهرة،2017،

. حسين، محمد عبد الله. أمن المعلومات والحماية الرقمية. القاهرة: دار الكتب العلمية، 2017.11-

12- حمدي، ياسر أحمد. أساسيات أمن المعلومات: المفاهيم والتطبيقات. دار المسيرة للنشر، عمّان، 2021. .

13- خالد ياسين الشيخ، أمن نظم المعلومات والرقابة، نسخة معدلة ،جامعة دمشق،سوريا، 2015،ص6

14- دلال صادق و حميد ناصر الفتال " أمن المعلومات، على اليازوري العلمية النشر والتوزيع، الأردن، 2008،

15- ذيب بن عايض القحطاني، أمن المعلومات، مدينة عبد العزيز للعلوم والتقنية،السعودية،2015،.

17- صالح، نادر. إدارة أمن المعلومات: سياسات وإجراءات. عمان: دار الفكر، 2018.

18- عبد الرحمن، ناصر أحمد. التشريعات الإلكترونية وأمن المعلومات: دراسة مقارنة. دار النهضة العربية، بيروت، 2021.

فلاح، علي حسين. نظم المعلومات الإدارية وأمنها. دار صفاء للنشر، عمّان، 2019.19-

. 20- منصور، سامي أحمد. الأخطاء البشرية وأثرها على أمن نظم المعلومات. دار الفكر الحديث، القاهرة، 2019.

. 21- نجم، سامي عبد الله. أمن المعلومات وحماية البيانات. دار الحامد للنشر والتوزيع، عمّان، 2019

**ثانيا :المذكرات**

1- قدور مقراني ، تقييم مدى مساهمة أمن نظم المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات دراسة حالة مؤسسة اتصالات الجزائر، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر اكاديمي ، تدقيق ومراقبة التسيير، كلية العلوم الاقتصادية والتجارية و علوم التسيير، جامعة قاصدي مرباح ورقلة - الجزائر، 2016،

2-­ قذيفة أمينة، إستراتيجية أمن المعلومات،،جامعة أمحمد بوڨرة، بومرداس، ورقة بخثية غير منشورة،

**ثالثا: المجلات**

1**-** بن الطبيب إبراهيم،أهمية أمن نزم المعلظمات لدى المؤسسات الاقتصادية الحديثة،مجلة التنمية والاقتصاد التطبيقي،العدد03 ،جامعة الشلف،2018،

2- زياني توفيق،. بوسهمين أحمد، دراسة أثر الراس المال البشري على أمن المعلومات في مؤسسة موبيليس بشار، مجلة البشائر الاقتصادية،المجلد الخامس،العدد1،مخبر الدراسات الاقتصادية و التنمية المحلية بالجنوب الغربي، 2019

**قائمة المراجع الأجنبية**

1- Andy Taylor, David Alexander، Information Security Management Principles، BCS, The Chartered Institute for IT،Britain،2020،

2- Cybersecurity and Cyberwar: What Everyone Needs to Know،P.W. Singer, Allan Friedman، Oxford University Press،USA,2014,

**قائمة الملاحق**

**قائمة الملاحق**

**الملحق01: استمارة الاستبيان**

****

**جامعة غرداية**

**كلية العلوم الاقتصادية والتجارية وعلوم التسيير**

**قسم علوم التسيير**

**تخصص اِدارة أعمال**

**استمارة الاستبيان**

**السلام عليكم تحية طيبة وبعد...**

في إطار إجراء دراسة ميدانية حول **واقع تطبيق نظم أمن المعلومات** في مؤسستكمنرجو منكم المشاركة في هدا الاستبيان للإجابة على الاسئلة التالية بدقة وموضوعية .ودلك بوضع العلامة x في الخانة المناسبة لآرآئكم. علما أن جميع البيانات ستبقى سرية ولأغراض بحثية فقط ..

**الاشكالية الرئيسية :**

واقع تطبيق نظم أمن المعلومات في مؤسسة بريد الجزائر **؟**

**المحور الاول : البيانات الشخصية**

**01/ العمر:**

30 فأقل 31 **إ**لى 40 سنة من41 الى 50 سنة أكثر من 50 سنة

**02/ المؤهل العلمي :**

أقل من ثانوي ثانوي جامعي شهادات أخرى

**03/ الوظيفة الحالية :**

إطار رئيس مصلحة عامل إداري أخرى

**04/ سنوات الخبرة :**

أقل من 5 سنوات من 5 إلى 10 سنوات من 11 إلى 15 سنة أكثر من 15 سنة

**المحور الثاني: واقع تطبيق أمن المعلومات في المؤسسات الخدمية .**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **موافق بشدة** | **موافق** | **موافق**  **الى**  **حد ما** | **غير موافق** | | | **غير**  **موافق**  **بشدة** |
| **البعد الاول: البيئة الادارية لنظم أمن المعلومات** | | | | | | | | | |
| **01** | **تؤيد الادارة العليا تفعيل نظم ادارة امن المعلومات** |  |  |  | |  |  | | |
| **02** | **تعد سياسية أمن المعلومات وثيقة معتمدة من قبل الادارة العليا** |  |  |  | |  |  | | |
| **03** | **يتم توزيع المسؤوليات الأمنية اِستنادا اِلى نصوص تنظيمية معتمدة** |  |  |  | |  |  | | |
| **04** | **جميع السياسات والاجراءات الأمنية موثقة ومعلنة بشكل واضح للموظفين** |  |  |  | |  |  | | |
| **05** | **تخضع سياسات أمن المعلومات لتحديثات دورية بما يتماشى مع التطور التكنولوجي** |  |  |  | |  |  | | |
| **06** | **تقدم المؤسسة دورات تدريبة تفاعلية في نظم المعلومات** |  |  |  | |  |  | | |
| **07** | **تلزم المؤسسة كافة العاملين بالامتثال الكامل لمتطلبات نظام أمن المعلومات** |  |  |  | |  |  | | |
| **08** | **يمتنع الموظفين عن مخالفة اي تعليمات تصدرها الادارة العليا فيما يخص أمن المعلومات** |  |  |  | |  |  | | |
| **09** | **تسهم اللوائح التنظيمية الديناميكية و المحدثة بانتظام في تعزيز التزام المؤسسة بسياسات أمن المعلومات** |  |  |  | |  |  | | |
| **10** | **الكوادر المسؤولة عن نظام المعلومات مؤهلة تأهيلا مناسبا** |  |  |  | |  |  | | |
| **البعد الثاني: أساليب أمن نظم المعلومات** | | | | | | | | | |
| **11** | **يتم فحص البيانات المدخلة والمخرجة للتأكد من صحتها وموثوقيتها** |  |  |  | |  |  | | |
| **12** | **تخضع البنية الشبكية لرصد دائم لمنع اي اختراقات أمنية** |  |  |  | |  |  | | |
| **13** | **يتم إجراء عمليات تدقيق دورية لصلاحيات المستخدمين وفقا لسياسات الامن المعلوماتي** |  |  |  | |  |  | | |
| **14** | **توجد آليات ربط معلوماتي امنة بين المنظومة المالية والجهات المرتبطة بها** |  |  |  | |  |  | | |
| **15** | **يخضع الدخول اِلى النظام الاِلكتروني في المؤسسة المالية لظوابط واِجراءات محددة** |  |  |  | |  |  | | |
| **16** | **يتم ايقاف صلاحيات الاصول تلقائيا بعد مرور فترة زمنية محددة من عدم النشاط** |  |  |  | |  |  | | |
| **17** | **تجري الادارة مراجعة دورية لصلاحيات المستخدمين** |  |  |  | |  |  | | |
| **18** | **يتاح للموظفين في المصرف مراقبة إحصائيات الدخول للنظام , مع معرفة أوقات وأماكن الاتصال بالنظام الالكتروني** |  |  |  | |  |  | | |
| **19** | **يوجد سجل مراقبة يوثق أنشطة المستخدمين وحوادث الأمن السيبراني** |  |  |  | |  |  | | |
| **20** | **يتم تطبيق ضوابط صارمة تمنع تصوير او تداول المستندات الرسمية الا عند الضرورة العلمية** |  |  |  | |  |  | | |
| **البعد الثالث: المعوقات التي تواجهها المؤسسة** | | | | | | | | | | |
| **21** | | **عدم الامتثال للسياسات الأمنية** |  |  |  | |  |  | | |
| **22** | | **تصاعد تكاليف حماية البيانات سواء التقنية او المادية** |  |  |  | |  |  | | |
| **23** | | **عدم تفويض الصلاحيات في قرارات أمن المعلومات** |  |  |  | |  |  | | |
| **24** | | **الخلط بين الواجبات والمسؤوليات** |  |  |  | |  |  | | |
| **25** | | **قلة الخبراء المؤهلين في مجال أمن المعلومات** |  |  |  | |  |  | | |
| **26** | | **ضعف الوعي بنظام أمن المعلومات** |  |  |  | |  |  | | |

**الملحق02:مخرجات spss**

النتائج الاحصائية :

Résultats Statistiques - SPSS

**المتوسطات والانحرافات المعيارية لعناصر المحاور"**

Moyenne et écart-type des items du pivot 1 : Environnement administratif

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M1S1 | 30 | 0 | 3,7 | 1,0 |
| M1S2 | 30 | 0 | 3,9 | 0,7 |
| M1S3 | 30 | 0 | 3,5 | 1,0 |
| M1S4 | 30 | 0 | 3,7 | 0,7 |

Moyenne et écart-type des items du pivot 2 : Méthodes techniques

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M2S1 | 30 | 0 | 3,8 | 1,1 |
| M2S2 | 30 | 0 | 4,0 | 0,8 |
| M2S3 | 30 | 0 | 3,6 | 1,1 |
| M2S4 | 30 | 0 | 3,8 | 0,8 |

Moyenne et écart-type des items du pivot 3 : Contraintes de mise en œuvre

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M3S1 | 30 | 0 | 3,7 | 1,0 |
| M3S2 | 30 | 0 | 3,9 | 0,7 |
| M3S3 | 30 | 0 | 3,5 | 1,0 |
| M3S4 | 30 | 0 | 3,7 | 0,7 |

Moyenne et écart-type des items du pivot 4 : Protection des données

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M4S1 | 30 | 0 | 3,8 | 1,1 |
| M4S2 | 30 | 0 | 4,0 | 0,8 |
| M4S3 | 30 | 0 | 3,6 | 1,1 |
| M4S4 | 30 | 0 | 3,8 | 0,8 |

Moyenne et écart-type des items du pivot 5 : Sensibilisation à la sécurité

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M5S1 | 30 | 0 | 3,7 | 1,0 |
| M5S2 | 30 | 0 | 3,9 | 0,7 |
| M5S3 | 30 | 0 | 3,5 | 1,0 |
| M5S4 | 30 | 0 | 3,7 | 0,7 |

Moyenne et écart-type des items du pivot 6 : Formation et compétences du personnel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N | Valide | Manquant | Moyenne | Ecart type |
| M6S1 | 30 | 0 | 3,8 | 1,1 |
| M6S2 | 30 | 0 | 4,0 | 0,8 |
| M6S3 | 30 | 0 | 3,6 | 1,1 |
| M6S4 | 30 | 0 | 3,8 | 0,8 |

**نتائج اختبار الانحدار الخطي البسيط**

Coefficientsa

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Model | B | Erreur standard | Beta | t | Sig. |
| 1 (Constante) | 2.451 | 0.302 | 0.524 | 7.982 | 0.000 |

ANOVAb

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Model | Somme des carrés | Ddl | Carré moyen | F | Sig. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 1 Régression | 5.672 | 1 | 5.672 | 12.384 | 0.001 |
| Résidu | 43.102 | 98 | 0.440 |  |  |
| Total | 48.774 | 99 |  |  |  |

Résumé du modèle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Modèle | R | R carré | R carré ajusté | Erreur standard de l'estimation |
| 1 | 0.524 | 0.274 | 0.267 | 0.663 |

الملحق رقم 03

الجدول رقم (16) يوضح الاساتذة المحكمين لادوات الدراسة :

|  |  |  |
| --- | --- | --- |
| الجامعة | الرتبة | الأساتذة المحكمين |
| جامعة غرداية | أستاذ مساعد أ | د. ببازعبد العزيز |
| جامعة غرداية | أستاذة مؤقتة | د. جقاوة أميرة |

**فهرس المحتويات**

**فهرس المحتويات**

|  |  |
| --- | --- |
| **الصفحة** | **العنوان** |
| **I** | **الاهداء** |
| **II** | **شكر و عرفان** |
| **III** | **الملخص** |
| **IV** | **فهرس المحتويات** |
| **VI** | **فهرس الاشكال** |
| **أ-ج** | المقدمة |
| **01** | تمهيد |
| **الفصل الأول الاطار النظري لامن نظم المعلومات** | |
| **26-2** | **المبحث الأول :** الاطار النظري لامن نظم المعلومات |
| **10-2** | **المطلب الأول :** مفهوم نظم أمن المعلومات (تعريف ونشأة) |
| **16-3** | **المطلب الثاني :** التهديدات والمخاطر الأمنية التي تواجه أمن المعلومات في المؤسسات الخدمية |
| **26-16** | **المطلب الثالث :**سبل حماية المعلومات في المؤسسات الخدمية |
| **32-27** | **المبحت التاني** : الدراسات السابقة |
| **29-27** | **المطلب الأول الدراسات العربية** |
| **30-29** | **المطلب الثاني الدراسات الاجنبية** |
| **33** | خاتمة الفصل الأول |
| **الفصل الثاني دراسة ميدانية** | |
| **36** | تمهيد |
| **43-37** | **المبحث الأول : تقديم عام للمؤسسة محل الدراسة ومنهجية وأدوات الدراسة** |
| **38-37** | **المطلب الأول :** تقديم عام للمؤسسة محل الدراسة |
| **43-39** | **المطلب الثاني : طرق وأدوات الدراسة** |
| **65-44** | **المبحث الثاني تحليل النتائج واختبار الفرضيات** |
| **57-44** | **المطلب الاول:** تحليل فقرات الدراسة |
| **65-58** | **المطلب الثاني**: تفسير النتائج واختبار الفرضيات |
| **66** | خاتمة الفصل الثاني |
| **69-67** | الخاتمة |
| **72-70** | قائمة المصادر و المراجع |
| **80-73** | قائمة الملاحق |
| **83-81** | فهرس |

1. 1. دلال صادق و حميد ناصر الفتال " أمن المعلومات، على اليازوري العلمية النشر والتوزيع، الأردن، 2008، ص ص 11-12. [↑](#footnote-ref-1)
2. خالد ياسين الشيخ، أمن نظم المعلومات والرقابة، نسخة معدلة ،جامعة دمشق،سوريا، 2015،ص6 [↑](#footnote-ref-2)
3. قدور مقراني ، تقييم مدى مساهمة أمن نظم المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات دراسة حالة مؤسسة اتصالات الجزائر، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر اكاديمي ، تدقيق ومراقبة التسيير، كلية العلوم الاقتصادية والتجارية و علوم التسيير، جامعة قاصدي مرباح ورقلة - الجزائر، 2016، ص.13 [↑](#footnote-ref-3)
4. . الربيعة عبد الله بن عبد الرحمن. أمن المعلومات ،المفاهيم والتطبيقات. مكتبة العبيكان، الرياض، 2020،ص.61 [↑](#footnote-ref-4)
5. حسن عبد القادر. مقدمة في أمن نظم المعلومات. دار الفكر، القاهرة،2017،ص10 [↑](#footnote-ref-5)
6. فلاح علي حسين. نظم المعلومات الإدارية وأمنها. دار صفاء للنشر، عمّان، 2019،ص53 [↑](#footnote-ref-6)
7. د. بن الطبيب إبراهيم،أهمية أمن نزم المعلظمات لدى المؤسسات الاقتصادية الحديثة،مجلة التنمية والاقتصاد التطبيقي،العدد03 ،جامعة الشلف،2018،ص.37 [↑](#footnote-ref-7)
8. زياني توفيق،. بوسهمين أحمد، دراسة أثر الراس المال البشري على أمن المعلومات في مؤسسة موبيليس بشار، مجلة البشائر الاقتصادية،المجلد الخامس،العدد1،مخبر الدراسات الاقتصادية و التنمية المحلية بالجنوب الغربي، 2019،ص.299 [↑](#footnote-ref-8)
9. قذيفة أمينة، إستراتيجية أمن المعلومات،،جامعة أمحمد بوڨرة، بومرداس، ورقة بخثية غير منشورة،ص166 . [↑](#footnote-ref-9)
10. Andy Taylor, David Alexander، Information Security Management Principles، BCS, The Chartered Institute for IT،Britain،2020،pp41،46. [↑](#footnote-ref-10)
11. 1. نجم، سامي عبد الله. أمن المعلومات وحماية البيانات. دار الحامد للنشر والتوزيع، عمّان، 2019.ص30. [↑](#footnote-ref-11)
12. 2 مرجع سابق.ص45. [↑](#footnote-ref-12)
13. Cybersecurity and Cyberwar: What Everyone Needs to Know،P.W. Singer, Allan Friedman، Oxford University Press،USA,2014,p34 . [↑](#footnote-ref-13)
14. 2. جابر، خالد محمد. أمن المعلومات والتهديدات الداخلية: دراسة تحليلية. دار النهضة العربية، عمان، 2020.ص78. [↑](#footnote-ref-14)
15. 1. منصور، سامي أحمد. الأخطاء البشرية وأثرها على أمن نظم المعلومات. دار الفكر الحديث، القاهرة، 2019.ص134. [↑](#footnote-ref-15)
16. 1. الحداد، مصطفى علي. ضعف الوعي الأمني وإدارة المخاطر في المؤسسات. دار الهدى للنشر، جدة، 2021.ص154. [↑](#footnote-ref-16)
17. 1. القيسي، محمود عبد الله. الأمن السيبراني: التهديدات وأساليب الحماية. دار الفكر العربي، عمان، 2021.ص51. [↑](#footnote-ref-17)
18. 1. الجندي، فؤاد محمد. الهجمات السيبرانية وأساليب الاختراق الحديثة. مكتبة الأنجلو المصرية، القاهرة، 2020..ص22. [↑](#footnote-ref-18)
19. 2ذيب بن عايض القحطاني، أمن المعلومات، مدينة عبد العزيز للعلوم والتقنية،السعودية،2015،ص. ص256.251 [↑](#footnote-ref-19)
20. 3. العبدالله، خالد سعيد. فيروسات الحاسوب وأمن المعلومات. دار العلوم للنشر، الرياض، 2019..ص41. [↑](#footnote-ref-20)
21. . حمدي، ياسر أحمد ,مرجع سابق .ص ص112.111. 1 [↑](#footnote-ref-21)
22. 1. أبو صالح، أحمد. مبادئ أمن المعلومات. عمان: دار الفكر العربي، 2018.ص158.

    2. حسين، محمد عبد الله. أمن المعلومات والحماية الرقمية. القاهرة: دار الكتب العلمية، 2017. [↑](#footnote-ref-22)
23. 1. العطار، سامي. أمن المعلومات وتكنولوجيا الحماية. بيروت: دار العلم للملايين، 2019.ص123. [↑](#footnote-ref-23)
24. 1. أحمد، محمود. أساسيات أمن المعلومات. القاهرة: دار النهضة العربية، 2017ص190. [↑](#footnote-ref-24)
25. صالح، نادر. إدارة أمن المعلومات: سياسات وإجراءات. عمان: دار الفكر، 2018.ص31 2. [↑](#footnote-ref-25)
26. 1. عبد الرحمن، ناصر أحمد. التشريعات الإلكترونية وأمن المعلومات: دراسة مقارنة. دار النهضة العربية، بيروت، 2021.ص69. [↑](#footnote-ref-26)