جامعة قاصدي مرباح – ورقلة–

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

مذكرة تخرج لنيل شهادة الماستر الأكاديمي

الميدان:علوم إنسانية

الشعبة:علوم الإعلام والاتصال

تخصص:اتصال جماهيري والوسائط الجديدة

إعداد الطالبة:بن قنان أسماء

إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية

دراسة ميدانية بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي- ورقلة-.

نوقشت وأجيزت علنا بتاريخ:2024/06/05

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
أد عبد القادربودربالة	أستاذ	جامعة ورقلة	رئيسا
د.جيتي نادية	أستاذ محاضر أ	جامعة ورقلة	مشرفا ومقررا
د.صانع رابح	أستاذ محاضر أ	جامعة ورقلة	مناقشا

السنة الجامعية:2024/2023

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

Université Kasdi Merbah - Ouargla
Faculté des Sciences
Humaines Et sociales
Département des Sciences de
l'information et de la communication

جامعة قاصدي مرباح ورقلة
كلية العلوم الإنسانية والاجتماعية
قسم علوم الاعلام والاتصال

تصريح شرفي
بالالتزام بمعايير الأمانة والنزاهة العلمية في إعداد مذكرة الماستر

أنا الممضي أسفله:

الطالب (ة): بحة قنايدة اسماء .....

المولود (ة) في: 15/12/2000 ..... بـ: ورقلة .....

الحامل لبطاقة التعريف (ر/س) رقم: 200213651 الصادرة بتاريخ: 10/12/2017

عن: ..... /

المسجل بالسنة: **الثانية ماستر** شعبة: **علوم الاعلام والاتصال**

تخصص: **الاتصال الجماهيري والوسائط الجديدة** [X] **سمعي بصري** [ ]

خلال السنة الجامعية: 2024/2023.....

والمعد لمذكرة الماستر التي تحمل عنوان: إستراتيجية الأمن المعلوماتي في المؤسسات العمومية الجزائرية جزائرية ميدانية في الوكالة الوطنية لتسيير القرض المصغر القرع اليهودي ورقلة .....

أصرح بشرفي أني التزمت بمراعاة معايير الأمانة والنزاهة العلمية المطلوبة في انجاز مذكرة الماستر المذكورة أعلاه

حرر بتاريخ: 22 ماي 2024

التوقيع والبصمة

جامعة قاصدي مرباح – ورقلة–

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

مذكرة تخرج لنيل شهادة الماستر الأكاديمي

الميدان:علوم إنسانية

الشعبة:علوم الإعلام والاتصال

تخصص:اتصال جماهيري والوسائط الجديدة

إعداد الطالبة:بن قنان أسماء

إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية

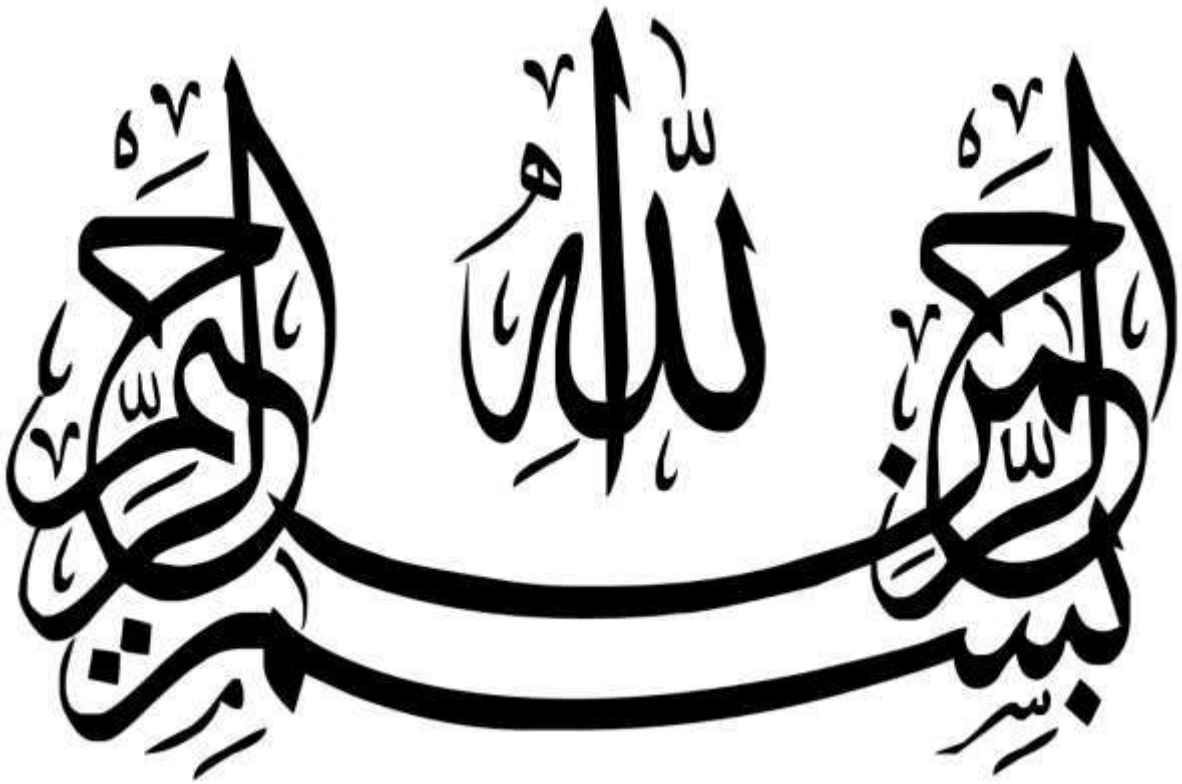
دراسة ميدانية بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي- ورقلة-.

نوقشت وأجيزت علنا بتاريخ:.....

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
أ.دعبدالقادربودربالة	أستاذ	جامعة ورقلة	رئيسا
د.جيتي نادية	استاذ محاضر أ	جامعة ورقلة	مشرفا ومقررا
د.صانع رابح	استاذ محاضر أ	جامعة ورقلة	مناقشا

السنة الجامعية:2024/2023


بسم الله الرحمن الرحيم

قال ابن خلدون:

"لابد للعمران البشري من سياسة ينتظم بها أمره"

شكر وعرفان

الحمد لله الذي علَّمَ بالقلم، علَّم الإنسانَ ما لم يعلَم

والصَّلاة والسَّلام على النبي الأكرَم،نبيِّنا ومعلمنا محمد – صلَّى الله عليه وعلى آله وصحبه وسلَّم.

أما بعد :عرفانا بحسن الصنيع والفضل الجميل، أتقدم بجزيل الشكر

وبكثير من الامتنان إلى أخي "د.بن قنان مسعود" على دعمه المعنوي

ومعلوماته القيمة التي أفادني بها أدامه الله

كما لا أنسى بالذكر مديرة الوكالة الوطنية لتسيير القرض المصغر

الفرع الجهوي ورقلة جزاها الله خيرا

ثم الشكر لكل إنسان أمد لي يد المساعدة من قريب أو بعيد وأتقدم بوافر التقدير للأساتذة الكرام في لجنة المناقشة والتقييم واخص بالذكر

الأستاذة المشرفة"جيتي نادية"جزاها الله عني كل خير

وبارك الله في علمها وسدد خطاها

الإهداء

قال الله تعالى:(وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنين)

اهدي هذا العمل إلى.....

من كلله الله بالهيبة والوقار إلى من علمني العطاء بدون انتظار إلى من احمل اسمه بكل افتخار رحل قبل أن يراني أحقق حلمه

والدي الغالي رحمه الله.

إلى ملاكي في الحياة إلى معنى الحب والحنان والتفاني إلى بسمة الحياة وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي

إلى أغلى الحبايب أمي الغالية أطال الله في عمرها.

إلى نصفي الأخر إلى من يعطي للحياة نكهتها وللروح مداها وللقلب سكينته زوجي حفظه الله.

إلى مهجة قلبي وفرحة حياتي إلى من تعلم قواعد المنهجية وعلوم الإعلام والاتصال وهو في بطني قبل أن يرى النور صغيري "أحمد باسم".

إلى أجمل الأقدار من قال فيهما الرحمان:"سنشد عضدك بأخيك"

إليكم يا سندي في الحياة إخوتي :عبد القادر،

عبد المالك،فاطمة،فتيحة،عائشة،سمية،سعاد،مسعود،محمد

،لحسن(رحمه الله)،عمار،عبد الحفيظ

إلى زهور بيتنا:أبناء أخواتي وإخوتي حفظهم الله

"اللهم انفعنا بما علمتنا وزدنا علما"

ملخص الدراسة باللغة العربية:

انطلقت الدراسة التي بين أيدينا من إشكالية مفادها: ماهي إستراتيجية الأمن المعلوماتي التي تتبعها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة؟

خلصت الدراسة إلى أن : المؤسسة تعتمد على مجموعة من الأساليب للحماية المادية والبرمجية وأساليب للحماية التنظيمية والإدارية كما تضع سياسة أمنية خاصة بها،وتنسب مهمة حماية المعلومات والبيانات الحساسة في المؤسسة بالدرجة الأولى إلى الدائرة المكلفة بالإحصاء والإعلام الآلي يشرف على هذه الدائرة مهندس إحصاء، ومهندس إعلام ألي مهمته المحافظة على الأمن المعلوماتي للمؤسسة،ولكل دائرة في المؤسسة معلومات وبيانات خاصة بها،كماتختلف درجة حماية المعلومات بالمؤسسة باختلاف نوعيتها وأهميتها بينماتختلف درجة وعي الموظفين بأهمية الأمن المعلوماتي فيوجد موظفين لديهم درجة عالية من الوعي وهم المتمثلين في أصحاب الأقدمية المتخصصين في مجال الإعلام الآلي ،بينما هناك موظفين على درجة قليلة من الوعي تحرص المؤسسة في الأساس على أن لا تتوفر لديهم المعلومات الحساسة والسرية بل يمكن أن يحصلوا على معلومات سطحية لا تؤثر على الأمن المعلوماتي للمؤسسة.

الكلمات المفتاحية:الإستراتيجية،الأمن المعلوماتي،المؤسسة العمومية.

Abstract : The study at hand started from the problem: What is the information security strategy followed by the National Agency for Microcredit Management, Ouargla Regional Branch?

The study concluded that: The institution relies on a set of methods for physical and software protection and methods for organizational and administrative protection. It also sets its own security policy. The task of protecting sensitive information and data in the institution is attributed primarily to the department in charge of statistics and automated information. This department is supervised by a statistical engineer and a media engineer. Its mission is to maintain the information security of the institution, and each department in the institution has its own information and data. The degree of information protection in the institution varies according to its quality and importance, while the degree of employee awareness of the importance of information security varies. There are employees who have a high degree of awareness, and they are represented by those with seniority who specialize in the field of automated media, While there are employees with a low degree of awareness, the organization is primarily keen to ensure that they do not have access to sensitive and confidential information. Rather, they may obtain superficial information that does not affect the organization's information security.

Keywords: strategy, information security, public institution.

فهرس المحتويات:

فهرس الجداول

فهرس الأشكال البيانية

مقدمة

مقدمة:

يعتبر أمن المعلومات تحديا هاما في مجال التكنولوجيات الجديدة للمعلومات. و بحكم المكانة الهامة التي تحتلها هذه الأخيرة في المجتمعات الحديثة، توسّع مجال أمن المعلومات حاليا إلى ميادين الأنظمة و المحتويات و الخدمات، و ذلك بهدف الوقاية من الهجمات و تحديدها و تقليصها في هذه الميادين . وتتمثّل مهمة أمن المعلومات في ضمان سلامة و سرية و توفر و سهولة تعقب البيانات و معالجاتها.

إن الأمن عنصر أساسي في كافة الأنظمة المعلوماتية. و يتمثل الهدف الأساسي لقسم الأمن المعلوماتي في اكتساب الخبرات و اقتراح الحلول من أجل ضمان السير الحسن لنظم الكمبيوتر و حمايتها من الاختراقات،[1]هذا ما جعل مؤسسات الأعمال تتجه إلى استخدامه للاستفادة من المزايا التي يوفرها فيما يتعلق بتحسين أدائها وربح الوقت في إدارة معلوماتها،خاصة في وقتنا الحاضر أين أخذت المعلومات دورا أكثر عمقا وشمولية واكتسبت بفعل ذالك قدرا يفوق كثيرا ما كانت تمثله من أهمية في وقت مضى ،وهذا بفضل اندماج تكنولوجيا الاتصال مع تكنولوجيا المعلومات وما صاحبها من تطور لنظم استغلالها ،حيث عرف نظام المعلومات الذي يعد المسئول الأول عن إنتاج المعلومات بالمؤسسة تطورا ت منذ ظهوره حتى الآن ،بالاعتماد على تكنولوجيا المعلومات والاتصال خاصة منها لشبكات الداخلية وشبكة الانترنت التي سمحت بتطوير جملة الخدمات التي يوفرها هذا النظام والتي تمكن المؤسسة من استغلال أمورها بشكل أفضل.

لكن هذا الاستخدام يحمل الكثير من المخاطر والتهديدات التي قد تؤثر على سير العمل ،وتصاحبه جملة من التهديدات والاعتداءات الالكترونية التي تلحق أضرارا بالغة بالمؤسسة قد تصل إلى حد التلاعب بمعلوماتها وتخريبها[2] ،لهذا تلجا المؤسسات إلى وضع إستراتيجية أمنية لحماية معلوماتها وكذالك سياسة أمنية تنظم عمل أدارة معلوماتها،فالأمن المعلوماتي هو بمثابة صك الأمان للمؤسسة كونه العلم الذي يعنى بحماية المعلومات من مختلف المخاطر التي قد تتعرض مثل السرقة أو التخريب واو التعديل إلى غير ذالك ،إن المؤسسات العمومية الجزائرية كغيرها من المؤسسات العالمية تسعي لصياغة إستراتيجية أمنية محكمة وتنفيذها من أجل توفير الحماية اللازمة للمؤسسة من جميع المخاطر الأمنية والهجمات الالكترونية،التي تهددها وزيادة القدرة على مواجهتها وتأمين المعلومات السرية و المالية والشخصية وقواعد البيانات والملفات والأصول الحرجة للمعلوماتية(قواعد البيانات،الخوادم،شبكات المعلومات،أنظمة التشغيل،البرامج،أجهزة التخزين).ومن بين هذه المؤسسات العمومية الجزائرية نجد الوكالة الوطنية لتسيير القرض المصغروالتي تعتبر من أهم هياكل دعم

وتعزيز المؤسسات الصغيرة والمتوسطة في الجزائر حيث تهدف إلى منح قروض مصغرة إلى الشباب الراغب في إنشاء مشروع مصغر بالإضافة إلى تغطية القروض التي منحها البنك وذلك بهدف تشجيع هذه الأخيرة على منح الائتمان لتمويل عملية إنشاء المؤسسات المصغرة وتعتبر الوكالة الوطنية لتسيير القرض القرض المصغر الفرع الجهوي ورقلة فرع من فروع هذه المؤسسة . والتي تسعى بدورها كغيرها من الشركات إلى المحافظة على سرية معلوماتها وبياناتها الخاصة بها وبالموظفين والمتعاملين من الاختراق،وجاءت دراستنا هذه لتسليك الضوء أو لمعرفة إستراتيجية امن المعلومات التي إنشائها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة باعتبارها العنصر الحساس والأساسي للمؤسسة.ولكي يتسنى لنا تقديم دراسة منهجية قسمنا دراستنا إلى فصلين(الإطار المنهجي والجانب الميداني):

_الفصل الأول بعنوان الجانب المنهجي والنظري للدراسة قمنا فيه بصياغة إشكالية الدراسة وتساؤلاتها الفرعية بالإضافة إلى أهداف الدراسة و أهميتها ومن ثم تطرقنا إلى أسباب اختيار موضوع الدراسة،وكذا منهج الدراسة وأدوات جمع البيانات ،وحدود الدراسة الزمانية والمكانية والموضوعية،ثم قمنا بجمع مصطلحات ومفاهيم الدراسة ،ثم استعرضنا الدراسات السابقة التي قد تتشابه مع دراستنا،وأخير تطرقنا إلى المقاربة النظرية وقمنا بإسقاطها على الدراسة .

_الفصل الثاني:قسمناه إلى مجموعة من الباحث: المبحث الأول تحت عنوان إجراءات الدراسة ميدانيا والمبحث الثاني حول الإجراءات و الوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية معلوماتها،أما المبحث الثالث فكان عن الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة والمبحث الرابع كان عن البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها أما المبحث الخامس فكان حول المخاطر التي تهدد امن المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

1_مركز البحث في الإعلام العلمي والتقني،cerist . _https://www.cerist.dz/index. –

2_نوفيل حديد_كريبط حنان:امن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة،كلية العلوم الاقتصادية،العلوم التجارية وعلوم التسيير،جامعة الجزائر3،مجلة المؤسسة،العدد ،2004 ،ص187.

الفصل الأول :الإطار المنـهجي للدراسة

1_ صياغة إشكالية الدراسة وتساؤلاتها الفرعية

2_ أهداف الدراسة

3_ أهمية الدراسة

4_ أسباب اختيار الموضوع

5_ منهج الدراسة وأدوات جمع البيانات

6_ حدود الدراسة

7_مصطلحات ومفاهيم الدراسة

8_ الدراسات السابقة

9_ المقاربة النظرية للدراسة

الإشكالية:

يعد مجال أمن المعلومات واحدا من أهم المجالات في الوقت الحالي ولا سيما للوظائف التي تتسم بياناتها بالسرية والخصوصية إذ يقوم هذا العلم على حماية هذه المعلومات والحفاظ على خصوصيتها ضمن نطاق الأشخاص المسموح لهم فقط ويمكن القول بأن هذا المجال هو فرع من فروع العلوم التقنية الحديثة وفيه يتم حماية المعلومات والبيانات المتداولة سواء على الانترنت أو المحفوظة بشكل رقمي في مركز البيانات من الهجمات الضارة أو الوصول الغير مسموح لأي طرف خارجي أو التعرض للتخريب ويوفر نظام أمن المعلومات الحماية المطلوبة للمعلومات المالية والشخصية والمعلومات الحساسة أو السرية المُخزنة في كل من الأشكال الرقمية والمادية، وبالتالي فهو يغطي مجموعة من مجالات تكنولوجيا المعلومات، ومنها البنية التحتية وأمن الشبكة والتدقيق والاختبار.[1]

ومن أهم عوامل الحفاظ على امن المعلومات هو وضع سياسات وإجراءات كافية لحمايتها فإستراتيجية الأمن هي أساس الأمن المعلوماتي في أي مؤسسة والتي باتت يوما بعد الأخر تدرك أهمية حماية بياناتها أكثر من أي وقت مضى ،خاصة في ظل العصر الرقمي الذي نعيشه حاليا والذي يشهد زيادة غير مسبوقة في أعداد الجرائم الالكترونية .فأمن المعلومات هو بمثابة الجهاز العصبي لأي مؤسسة حيث إن وجود عطل أو خلل به يتسبب في العديد من الأضرار الخاصة بمختلف الأقسام فهو عبارة عن أداة تضمن سرية المعلومات الخاصة بالمؤسسة وتعمل على توافرها وتضمن مصداقيتها وهذا يقلل من حدوث أزمات في الشركة وإستراتيجية الأمن هي السياسة والأدوات التي تم تصميمها واستخدامها في حماية جميع البيانات من التعطيل والسرقة والتدمير،إن السياسة المنفذة بشكل جيد تحتوي معلومات كافية لما يجب فعله لحماية المعلومات والعاملين في المؤسسة،ولتجنب المخاطر الأمنية وجب وضع خطة محكمة ،بالإضافة إلى تفاعل جميع موظفي المنظمة والذي سيؤدي بدوره إلى نجاح إدارة امن المعلومات في المؤسسة.إن المؤسسات العمومية الجزائرية كغيرها من المؤسسات العالمية تسعي لصياغة إستراتيجية أمنية محكمة وتنفيذها همن أجل توفير الحماية اللازمة للمؤسسة من جميع المخاطر والهجمات السبرانية التي تهددها وزيادة القدرة على مواجهتها وتأمين المعلومات السرية و المالية والشخصية والمعلومات الحساسة المخزنة في كل من الأشكال الرقمية والمادية.ومن بين هذه المؤسسات العمومية الجزائرية نجد الوكالة الوطنية لتسيير القرض المصغروالتي تعتبر من أهم هياكل دعم وتعزيز المؤسسات الصغيرة والمتوسطة في الجزائر

حيث تهدف إلى منح قروض مصغرة إلى الشباب الراغب في إنشاء مشروع مصغر بالإضافة إلى تغطية القروض التي منحها البنك

وذلك بهدف تشجيع هذه الأخيرة على منح الائتمان لتمويل عملية إنشاء المؤسسات المصغرة وتعتبر الوكالة الوطنية لتسيير القرض القرض المصغر الفرع الجهوي ورقلة فرع من فروع هذه المؤسسة . والتي تسعى بدورها كغيرها من الشركات إلى المحافظة على سرية معلوماتها وبياناتها الخاصة بها وبالموظفين والمتعاملين من الاختراق.

تساؤلات الدراسة:

ومن هذا المنطلق نسعى في دراستنا إلى الإجابة عن التساؤل الرئيسي التالي:ماهي إستراتيجية الأمن المعلوماتي التي تتبعها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة؟

ويتفرع عنه جملة التساؤلات التالية:

1 _فيما تتمثل مجموعة الإجراءات والوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية بياناتها؟

2_من هي الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهري ورقلة؟

3_ما هي البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها؟

4_هل يمتلك الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة وعيا بضرورة المحافظة على الأمن المعلوماتي بمؤسستهم؟

1_اعمل بزنس ،امن المعلومات:المفهوم،العناصر،التهديدات،ووسائل الحماية،22اكتوبر2022.

https://www.e3melbusiness.com/blog/Information-Security

2_أهداف الدراسة:

_التعرف على الإجراءات والوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية بياناتها.

_معرفة الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهري ورقلة

_معرفة البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها.

_معرفة درجة ثقافة الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة بضرورة الأمن المعلوماتي.

3_أهمية الدراسة:

تنبع أهمية الدراسة من اهمية الموضوع الذي تتناوله وهو"الامن المعلوماتي" حيث تعتبر دراستنا كإضافة نوعية للرصيد العلمي والمعرفي بالإضافة إلى ذالك فإنها تعتبر كإضافة علمية في مجال علوم الإعلام والاتصال وكذا تتجلى أهمية هذه الدراسة من الجانب العلمي من خلال الأهمية البالغة التي يتحلى بها موضوع الأمن المعلوماتي في عصرنا الحالي ،إذ إن العديد من المؤسسات والمنظمات تعطي أهمية بالغة لحماية معلوماتها من الاختراق . وتعتبر هذه الدراسة إثراء لمكتبة قسم علوم الإعلام والاتصال بجامعة قاصدي مرباح ورقلة نظرا لندرة مثل هذه الدراسات التي تعالج موضوع الأمن المعلوماتي بالمؤسسات العمومية الجزائرية في القسم.

4_أسباب اختيار الموضوع:

_وقع اهتمامنا على هذا الموضوع كون الأمن المعلوماتي أضحى هاجس يؤرق المؤسسات وكذا الأفراد وذالك خشية التعرض إلى الاختراق .

_الفضول الذاتي تجاه كل ما تعلق بالمعلوماتية والمعلومات.

_الرغبة في التعرف على المشاكل التي تتعرض لها أنظمة المعلومات في المؤسسات العمومية .

_تقييم مدى كفاءة وفعالية نظام امن المعلومات في المؤسسات العمومية الجزائرية .

_دراسة موضوع الأمن المعلوماتي من اتجاه تخصص الإعلام والاتصال .

_ إثراء المعارف الشخصية ومكتبة الإعلام والاتصال والمؤسسة محل الدراسة

_إشباع الفضول العلمي لمعرفة مختلف الإجراءات والوسائل وطرق الحماية وكذا الإستراتيجية الأمنية بالدرجة الأولي التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر لحماية بياناتها.

_قابلية دراسة الموضوع من الناحية النظرية والتطبيقية.

_تزايد اهتمام المؤسسات بالأمن المعلوماتي وضرورة وضع إستراتيجية لحماية المعلومات.

5_مصطلحات ومفاهيم الدراسة:

الإستراتيجية:

لغة:الإستراتيجية في اللغة العربية ترجمة لمصطلح Strategyالموجودة في اللغة الإنجليزية،وهي تقابل مصطلح Strategicبالغة الفرنسية وStrategos في اللغة اليونانية تاريخيا،والتي كانت تعني فن قيادة القوات وإدارة العمليات الحربية.[1] تمثل وثيقة رسمية تعكس فلسفة وأفعال المنظمة وخططها التي ينبغي تبنيها لغرض تحقيق رؤيتها المستقبلية .[2] وهي شيء ديناميكي ومعقد قد تكون إستراتيجية ما ذات فائدة في يوم ما وعديمة الفائدة في اليوم التالي.[3]

أمن المعلومات :

الأمن لغة:من الأمان و الأمانة بمعنًى ،و قد أَمنتُ فأنا أَمنٌ ،وآمنتُ غيري من الأمْنِ و الأمان ، و الأمْن ضد الخوف ،و الأمانة ضد الخيانة ،وفي التنزيل العزيز: {وآمَنهُم مِّنْ خَوْف } فالأمْنُ نقيض الخوف . [4]

الأمن المعلوماتي Information Security :

يعتبر الكثير من الباحثين أن استخدام مصطلح امن المعلومات sécurité de linformationتم تداوله قديما قبل ولادة وسائل تكنولوجيا المعلومات،إلا انه وجد استخدامه الشائع بالطريقة الصحيحة والفعلية في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال.[5]

1_صلاح عبد القادر النعيمي،الإستراتيجية والإدارة الإستراتيجية نظرة تحليلية وعلاقات تكاملية للمفاهيم والمصطلحات،دار اليازوري للنشر والتوزيع 17،2021

2_عدنان مصطفى البار،خالد علي المرحبي:أمن المعلومات والأمن السيبراني، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز،ص10/1.

3_حكمت رشيد سلطان،محمود محمد أمين عثمان :الإدارة الإستراتيجية، شركة دار الأكاديميون للنشر والتوزيع،2019،ص12

4_ابن منظور،لسان العرب:المجلد الأول،دار الحديث ،القاهرة،2003،ص232.

5_بوازدية جمال،الأمن السيبراني،محاضرات مقدمة لطلبة السنة الثانية ماستر تخصص دراسات إستراتيجية وأمنية،جامعة الجزائر-3-كلية العلوم السياسية والعلاقات الدولية،2020-2021،ص26.

الأمن المعلوماتي من الزاوية التقنية: هو مجموعة الوسائل والتقنيات،والأدوات والإجراءات التقنية التي تسمح بحماية موارد النظام المعلوماتي ،من اجل ضمان توافر المعلومات ،سريتها وسلامة محتواها.[2]

الأمن المعلوماتي من الزاوية الأكاديمية:هو مجموعة الإجراءات والتدابير الوقائية التي تستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها السرقة أو الاختراق(Hack) فالمقصود بعلم أمن المعلومات هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات ويضع الأدوات والإجراءات اللازمة لضمان حمايتها.[3]

هو حماية المعلومات وأنظمة المعلومات من الدخول العشوائي(غير المراقب)، أو الاستخدام غير المرشد، أو الكشف عن تلك المعلومات لغير المعنيين،أو إفساد تلك المعلومات والتغيير والتعديل فيها وتشويهها وتدميرها، وذلك بغرض الحفاظ على المؤسسة و ثقة المستخدمين في المؤسسة.[4]

2_نوفيل حديد_كريبط حنان:امن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة،كلية العلوم الاقتصادية،العلوم التجارية وعلوم التسيير،جامعة الجزائر3،مجلة المؤسسة،العدد3،2004،ص186/207.

3_صلاح عبد القادر النعيمي،الإستراتيجية والإدارة الإستراتيجية نظرة تحليلية وعلاقات تكاملية للمفاهيم والمصطلحات،دار اليازوري للنشر والتوزيع 2021،ص16

4_ ولاء السيد عبدالله : إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي بمدارس التعليم الثانوي الصناعي ب ج.م، مجلة الإدارة التربوية ،العدد الثاني عشر – مارس2017 ،ص404/391

الأمن السيبراني:

وهي مأخوذة من كلمة(سيبر)وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني(فضاء الانترنت)،وهي كلمة مشتقة من الكلمة اليونانية Kybernetesالتي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة .[1]
و نعني به اتخاذ إجراءات،ووضع معايير لمنع وصول المعلومات الخاصة .أو لحماية تلك المعلومات بأن تكون في أيدي جهة معادية أشخاص غير مخولين بها عبر الشبكة المعلوماتية.والأمن في الفضاء السيبراني يتحقق فقط بوجود هذه الإجراءات.[2]

المؤسسات العمومية:

يقصد بالمؤسسة لغة : جمعية أو معهد أو شركة أسست لغاية علمية أو خيرية أو اقتصادية ... الخ[3]

أما كلمة عمومية فهي من فعل عم عموما : عم المطر الأرض، أي شملها، وعم القوم بالعطية أي شملهم .وعمم ضد خصص والعام خلاف الخاص، يقال: جاء القوم عامة، أي جميعا.[4]

هي منظمة إدارية عامة تتمتع بالشخصية القانونية وبالاستقلال المالي والإداري ترتبط بالسلطات الإدارية المركزية المختصة بعلاقات التبعية والخضوع للرقابة الإدارية الوصائية وهي تدار بالأسلوب الإداري اللامركزي لتحقيق أهداف محددة في نظامها القانوني.[5]

1_سعد علي الحاج علي بكري،» الأمن السيبراني ومعضلة حمايته ..عولمة التعليم العالي ..الرقمي« ، جريدة العرب الاقتصادية الدولية،العدد 25 ، 24 (أوت) 2017 ، ص 24..

2_Martin C.Libicki,Conquest in Cyberspace:National Security and Information Warfare.(New York:Cambridge University Press,2007) ,pp(1,14),on site:

3_المنجد في اللغة العربية، الطبعة 31، بيروت دار المشرق، 1991 ،ص11.

4_المنجد في اللغة العربية(نفس المرجع) .

5_إيمان بغدادي تطبيق قانون المنافسة على المؤسسة العمومية الاقتصادية ، مجلة التحولات الاقتصادية العدد: 02،المجلد:01،جامعة قسنطينة، ، 39 معهد العلوم الاقتصادية والتجارية وعلوم التسيير– المركز الجامعي مرسلي عبد الله . تيبازة، ص 30_31،dz edu .umc@baghdadi.imene .

المؤسسة العمومية الاقتصادية:

ورد التعريف بالمادة 02 من الأمر رقم 04-01 المؤرخ في 20 أوت 2001 ،يتعلق بتنظيم المؤسسة العمومية الاقتصادية وتسييرها وخوصصتها،بالنص: " المؤسسات العمومية الاقتصادية، هي شركات تجارية تحوز فيها الدولة أو أي شخص معنوي آخر خاضع للقانون العام، أغلبية رأس المال مباشرة أو غير مباشرة، وهي تخضع للقانون الخاص.[1]

التعاريف الإجرائية:

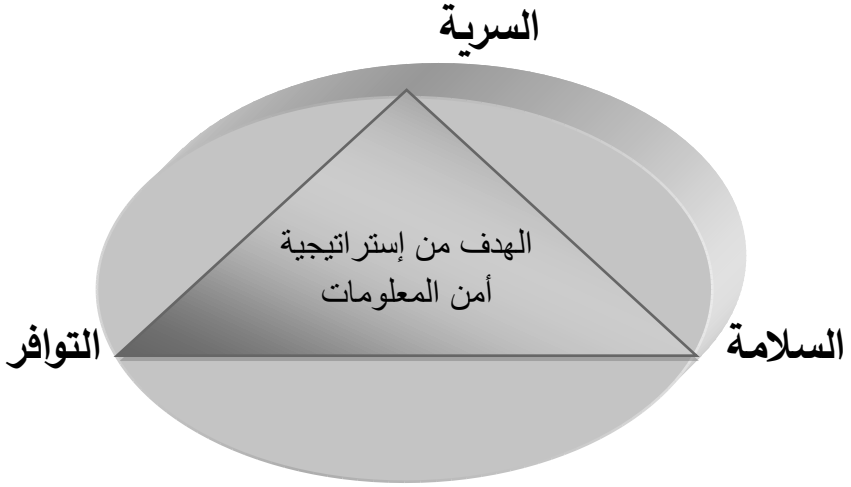
الأمن المعلوماتي: هوالحفاظ على المعلومات الخاصة بالمؤسسة وحمايتها من السرقة أو التعديل أو التغيير بدون إذن، أو الاستخدام غير المصرح به لهاته المعلومات.

إستراتيجية أمن المعلومات:

هي مجموعة القوانين المنظمة أو هي السياسة التي تتبعها المؤسسة تجاه أمن وحماية المعلومات في المؤسسة من جميع مصادر التهديد .

أو هي الخطة التي تعتمدها المؤسسة أو مجموعة القواعد التي تتعلق بوصول الأفراد إلى المعلومات والتصرف فيها.

الهدف من إستراتيجية أمن المعلومات في المؤسسة



1_ 22_عوابدي عمار،القانون الإداري ،الجزء الأول،ط5،ديوان المطبوعات الجامعية،2008 ،ص307.

الدراسات السابقة:

إن البحوث السابقة هي مصدر الهام لا غنى عنه بالنسبة للباحثين لان كل بحث هو امتداد للبحوث الذي سبقته لذالك لابد من استعراض الأدبيات السابقة ومعرفة الأعمال التي أنجزت من قبل حول الموضوع الذي نحن بصدد دراسته أو الأعمال التي تشبهه .

أولا:الدراسات الوطنية:

الخطر المعلوماتي ومسؤولية حماية المعلومة في المؤسسة الاقتصادية، آمال بن اعراب[1]،2021

انطلقت دراستها من الإشكالية التالية:ما مدى أهمية المعلومة في المؤسسة الاقتصادية؟ وما هي المعلومات الواجب حمايتها وإلى من تسند هذه المهمة الحساسة؟

توصلت الدراسة إلى أن: المؤسسات الاقتصادية الجزائرية محل الدراسة يسندون مهمة حماية معلوماتهم إلى المستويات الإدارية العليا بالدرجة الأولى نظرا لحساسية هذه المهمة والمتمثلة إما في إدارة مختصة ومسئولة عن ذلك، وإما مصلحة قواعد البيانات، أو الإطارات والمسئولين القائمين على المؤسسة بصفة عامة، وذلك لضبط وتحديد المعلومات المهمة والحساسة والعمل على التخطيط ووضع إستراتيجية أمنية للمعلومات، وفي ذات الوقت تتبع إستراتيجية المشاركة المفتوحة التي تقوم على إشراك مع الأفراد المنتمين للمؤسسة،وتحسيسهم بمسؤوليتهم تجاه الحفاظ على معلومات المؤسسة من خلال عدم كشف الأسرار المهنية واستراتيجيات المؤسسة، وعدم الإفصاح عن مخططاتها المستقبلية، فلقد أثبتت العديد من الدراسات التطبيقية وتجارب الشركات أهمية مشاركة الأفراد العاملين للحد من المقاومة وتحمل مسؤولية الحفاظ على المؤسسة، بحيث نجد 2 . 02 % من بين المؤسسات المدروسة يوافقون على إشراك كل الفاعلين في المؤسسة. كما تقر معظم المؤسسات الاقتصادية الجزائرية المبحوثة بأهمية كل أنواع المعلومات التقنية منها والتجارية وحتى الاقتصادية والمالية...، لذلك من الضروري توفير الحماية لها لكن بشكل متفاوت، إلا أن المعلومات و القدرات التي تمتلكها المؤسسة وتعطيها سبقا تنافسيا هي الأكثر أهمية و من الأجدر توفير الحماية لها أولا وبدرجة أشد مقارنة بالمعلومات الأخرى.

أوجه الاستفادة من الدراسة:

تطرقت الباحثة في هذا المقال إلى أهم العناصرالتي يمكن أن تحيط بموضوع بحثنا،

وتشتمل على أهم أبعاده العلمية وأبرز زواياه النظرية والميدانية.

وتتشارك مع دراستنا في نتائج البحث المتعلقة بالجهة المكلفة بحماية الأمن المعلوماتي بالمؤسسة،وتفاوت درجة حماية المعلومات حسب أهميتها .

ثانيا:الدراسات العربية.

واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها،أيمن محمد فارس الدنف2013. [2]

انطلق الباحث من إشكالية دراسة مفادها:يستطيع متخذي القرار في الإدارات العليا للكليات التقنية التعرف على واقع إدارة أمن نظم المعلومات و الوقوف على جوانب الخلل ومعالجة أو إيجاد حلول لقضايا أمن نظم المعلومات .ومن خلال ما سبق يمكن صياغة مشكلة الدراسة بالتساؤلات التالية:

1_ ما هو واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة ؟

2_ما هي سبل تطوير إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة؟

تهدف هذه الدراسة إلى:

_التعرف على واقع أمن نظم المعلومات في الكليات التقنية بقطاع غزة.

_الكشف عن مهددات أمن نظم المعلومات في الكليات التقنية بقطاع غزة.

_التحقق من فعالية أساليب أمن المعلومات المستخدمة .

_تحديد سبل تطوير إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وفق آراء المبحوثين.

_ بيان مدى استخدام التعهيد (الاستعانة بالأطراف الخارجية)في الكليات التقنية.

_ وضع مقترحات وتوصيات بشأن تطوير أمن نظم المعلومات في الكليات التقنية.

1_آمال بن اعراب،الخطر المعلوماتي ومسؤولية حماية المعلومة في المؤسسة الاقتصادية،جامعة الجزائر 3،مجلة المعيار،المجلد:25،العدد:55،2021 **9090 /00/9094النشر علي الخط 9042 /07/ 41 القبول /07/ 97 تاريخ الوصول 41 Received 41/07/9042 Accepted 97/07/9090 Published online 15/03/2021.**

2_أيمن محمد فارس الدنف: واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، الجامعة الإسلامية– غزة عمادة الدراسات العليا كلية التجارة قسـم إدارة الأعمال، قدمت هذه الدراسة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية بغزة – كلية التجارة،2013.

*وتوصلت الدراسة إلى مجموعة من النتائج أهمها :

– تتوفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة.

– تدرك الإدارات العليا للكليات التقنية أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة.

– تتفاوت الكليات التقنية مجتمع الدراسة في درجات استخدام تعهيد نظم معلوماتها.

– توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة

*وفي ضوء هذه النتائج فقد أوصى الباحث بالتالي :

– ضرورة الاستمرار بالاهتمام بالبنى التحتية لنظم المعلومات وتطويرها لتجاري المستحدثات التكنولوجية السريعة .

– ضرورة أن تقوم الكليات التقنية ببناء سياسات أمن نظم المعلومات الخاصة بها، والعمل على نشرها و تطبيقها، والقيام بتطويرها ومراجعتها و تقييم المخاطر بشكل دوري للوقوف على ما يمكن عمله و ايجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات.

– ينصح بأن تقوم الكليات التقنية بالاعتناء بدور أكبر بالتدريب و زيادة الموازنات المالية المخصصة لعمليات أمن المعلومات.

– ضرورة قيام الجهات الحكومية بإنشاء مركز متخصص يعنى بقضايا أمن المعلومات.

أوجه الاستفادة من هذه الدراسة:

ساعدتنا في وضع منهجية الدراسة و بناء المصطلحات والمفاهيم.

ثالثا:الدراسات الأجنبية.

Information security management in IGT and non IGT sector companies:Apreventive innovation perspective ,Mona Mirtsh,Knut Blind,Claudia Koch,Gabriele Dudek.[1]

_دراسة ل:مونا ميرتش،كنوت بليند، كلوديا كوش، غابريال دوديك، بعنوان إدارة امن المعلومات في شركات قطاع تكنولوجيا المعلومات والاتصالات:منظور الابتكار الوقائي.

_تسعى هذه الدراسة إلى توسيع المعرفة حول تنفيذ نظام إدارة امن المعلومات استنادا إلى المعيار الدولي ISO/IEC27001 .

_تهدف هذه الدراسة لاستكشاف سبب اختيار الشركات لاعتماد ISO/IEC2700 .(الدوافع)

،والتأثيرات التي تواجهها ،والعقبات التي تواجهها،وكيفية ارتباط هذه الجوانب بكيفية إدراك الشركات المتبنية للفائدة الشاملة لاعتماد ISO/IEC27001 ،(والذي يمثل المعيار الدولي الرائد لإدارة امن المعلومات تم إعداده لتوفير متطلبات إنشاء وتنفيذ وصيانة وتحسين نظام إدارة امن المعلومات بشكل مستمر).

_قام الباحثون:بدراسة مسحية ل806شركة ألمانية إما تدعي حصولها على شهادة . ISO/IEC27001 أو مدرجة في قاعدة بيانات الشهادات التي يمكن الوصول إليها بشكل عام.

_واعتمدوا على المقابلة حيث قامو بإجراء عشر مقابلات مع مختلف أصحاب المصلحة:شركات حاصلة على ISO/IEC27001 من عدة قطاعات،وهيئتين لإصدار الشهادات ،وممثل واحد عن الهيئة الألمانية.

_توصلت الدراسة إلى النتائج التالية:

_إن سرية المعلومات وسلامتها وتوافرها تعتبر من الأصول المهمة التي يجب على الشركات من جميع الأحجام والصناعات حمايتها.

_اعتماد ISO/IEC27001 .باعتباره المعيار الدولي الأكثر شيوعا منخفض بشكل مدهش .

_إن التأثيرات الوقائية والعقبات التشغيلية أمام الاستثمار هي وحدها التي تعمل بشكل كبير على تحسين التصور العام للفائدة من اعتمادISO/IEC2700 .

_بالنسبة للتأثيرات الأخرى الناشئة عن الضغوط المؤسسية والاعتبارات الاقتصادية ،يتوقع الباحثون ان تزداد أهميتها مع تركيز أصحاب المصلحة بشكل اكبر على الشركات التي تتخذ تدابير فعالة لحماية امن المعلومات .

أوجه الاستفادة من هذه الدراسة:

ساعدتنا في الوصول إلى نظرية الدراسة، وفي بناء الأسس المنهجية لدراستنا.

تتوافق مع دراستنا في أن سرية المعلومات وسلامتها وتوافرها تعتبر من الأصول المهمة التي يجب على الشركات من جميع الأحجام والصناعات حمايتها.

_1 Mona Mirtsh,Knut Blind,Claudia Koch,Gabriele Dudek ,Information security management in IGT and non IGT sector companies:Apreventive innovation perspective ,Bundesanstalt für Materialforschung und −prüfung (Federal Institute for Materials Research and−Testing — BAM), Berlin, Germany, Technische Universität Berlin, Berlin, Germany, Fraunhofer Institute of Systems and Innovation Research (ISI), Karlsruhe, Germany,ELSEVER,26/06/2021.

_www.elsevier.com/locate/cose

_ منهج الدراسة وأدوات جمع البيانات:

تنتمي هذه الدراسة التي بين أيدينا إلى الدراسات الوصفية كون المنهج الوصفي يتلاءم مع طبيعة موضوع دراستنا ، حيث يعرف المنهج الوصفي انه المنهج الذي يعتمد على دراسة الظاهرة كما توجد في الواقع ويهتم بوصفها كيفيا وكميا.[1] وهو احد أشكال التحليل والتفسير العلمي المنظم لوصف ظاهرة وتصنيفها وتحليلها وإخضاعها للدراسة الدقيقة[2] واعتمدنا خلال دراستنا هذه على المنهج الوصفي التحليلي والذي يمثل المنهج الوصفي المتعمق ، حيث يصف الباحث العلمي مختلف الظواهر والمشكلات العلمية ، ويحل المشكلات والأسئلة التي تقع ضمن دائرة البحث العلمي ، ثم يتم تحليل البيانات التي تم جمعها من خلال المنهج التحليلي الوصفي ، بحيث يمكن استخلاص الشرح والنتائج.[3]

يقتصر المنهج الوصفي التقليدي على دراسة بعض الظواهر التي تأخذ طابعًا اجتماعيًا وبشريًا ، لكن مفهوم النهج الوصفي التحليلي له آليات تمكين أكثر ، يمكن من خلالها دراسة المزيد من الموضوعات في البحث العلمي[4] وهذا الذي يخدم بحثنا الذي نعمل من خلاله على تحديد ومعرفة الظاهرة من خلال الوصف والتحليل لما يمتلكه من مرونة وشمولية لمعرفة المسببات التي أدت لحدوث الظاهرة.

و في دراستنا سنحاول وصف واقع معين يتمثل في إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية وذلك من خلال وصف و تحليل البيانات التي جمعناها من اجل الوصول إلى نتائج دقيقة.

1_سعد سلمان المشهداني،منهجية البحث العلمي،ط1،الأردن ،دار أسامة للنشر والتوزيع ،2019،ص126.

2_محمد عبد السلام،مناهج البحث في العلوم الاجتماعية والانسانية،مكتبة نور،2020،ص163.

3_محمد تيسير،ما هو المنهج الوصفي التحليلي، وأهم خطوات إعداده؟،المؤسسة العربية للعلوم والنشر والأبحاثhttps://blog.ajsrp.com.

4_تيسير محمد، المنهج الوصفي التحليلي،نفس المرجع.

تساهم طرق البحث العلمي في التعرف على الظاهرة المدروسة ووضعها في إطارها الصحيح من اجل الوصول إلى نتائج الدراسة وذالك من خلال إتباع منهج يتناسب مع طبيعة الدراسة لذالك اعتمدنا في دراستنا هذه على منهج دراسة الحالة والذي يعرف بأنه يقوم على اختيار حالة معينة يقوم الباحث بدراستها وتكون دراسة هذه الحالة بشكل مستفيض يتناول كافة المتغيرات المرتبطة بها وتناولها بالوصف الكامل والتحليل.[1]وهو أيضا عبارة عن تحليل تنظيمي لوضعية ما من اجل إيجاد الحلول ومعالجة المشاكل هذا وتستند دراسة الحالة إلى البرهنة واستخدام العقل والمنطق في اقتراح التشخيص الجيد والتحليل المناسب .[2]

يعني جمع البيانات العلمية المتعلقة بأية وحدة سواء أكانت فردا أو مؤسسة أو مجتمع ،لذالك اعتمدنا عليه في موضوع دراستنا الذي يدور حول إستراتيجية الأمن المعلوماتي التي تعتمد عليها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

أدوات جمع البيانات:

يتوقف نجاح الباحث في تحقيقه لأهداف بحثه من خلال استخدامه لمجموعة من الأدوات المناسبة لموضوع دراسته ولقد اعتمدنا في بحثنا على المقابلة كأداة رئيسية والاستبيان كأداة مساعدة.

المقابلة:تعد إحدى الأدوات المعتمد عليها في الدراسات الميدانية يحصل من خلالها الباحث على المعلومات بطريقة شفوية،أي هي محادثة موجهة بين الباحث والمبحوث بهدف الوصول إلى الحقيقة من اجل تحقيق أهداف الدراسة وتعتبر أكثر الوسائل استخداما في جمع البيانات في كثير من البحوث الإنسانية نظرا لمميزاتها ومرونتها.[3]

1_محمود احمد درويش،مناهج البحث في العلوم الإنسانية،مؤسسة الأمة العربية للنشر والتوزيع ،مصر ،2018،ص164.

2_د.احمد أبو اسعد،د.سلطان النوري،دراسة الحالة في إطار جديد،مركز ديبونو لتعليم التفكير عضو اتحاد الناشرين العرب،عمان/دبي،2016،ص24.

3_ محمد در ،مجلة الحكمة للدراسات التربوية والنفسية،أهم مناهج وعينات وأدوات

البحث العلمي،مؤسسة كنوز الحكمة للنشر والتوزيع،العدد9،الجزائر ،2017.ص309_323.

قمنا بالاعتماد على المقابلة كأداة بحث علمي رئيسية من اجل الحصول على اكبر قدر من المعلومات حول السياسة الأمنية ومختلف الوسائل والإجراءات التي تتبعها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لبناء إستراتيجية أمنية ناجحة .قمنا بهذه المقابلة مع مديرة الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة ،وكذا مع مهندس الإعلام الآلي بالمؤسسة وهو المسئول على المحافظة على الأمن التقني لمعلومات وبيانات المؤسسة،ومقابلة هاتفية مع مدير الوكالة الولائية لتسيير القرض المصغر بغرداية.

قسمنا المقابلة إلى 5 محاور:

المحور الأول: الإجراءات و الوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية بياناتها.

المحور الثاني: الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهري ورقلة.

المحور الثالث: البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها.

_**المحور الرابع:** المخاطر التي تهدد امن المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

الحور الخامس: مدى وعي الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة بالأمن المعلومات.

_ **الإستبانة**:هي قائمة تتضمن مجموعة من الأسئلة المعدة بدقة ترسل إلى عدد كبير من أفراد المجتمع الذين يكونون العينة الخاصة بالبحث.[1]

لجئنا إليها كأداة مساعدة لمعرفة درجة ثقافة الأمن المعلوماتي لدى الموظفين ،قمنا بمسح شامل لجميع الموظفين نظر لقلة عددهم المتمثل في15 مفردة.

1_مروان عبد المجيد إبراهيم،أسس البحث العلمي لإعداد الرسائل الجامعية ،مؤسسة الوراق ،عمان ،ط1،2000،ص165.

ولقد قمنا بتقسيم الاستبانة إلى محورين كل محور يحتوي على مجموعة من الأسئلة :

_**المحور الأول** :المصادر التي تسهم في تكوين ثقافة الأمن المعلوماتي لدى الموظفين بالوكالة.

_**المحور الثاني**:امتلاك الموظف لمعلومات حول أساليب وطرق الاختراق الالكترونية.

_ومحور يتعلق بالبيانات الشخصية.

مجتمع البحث وعينة الدراسة:

مجتمع البحث هو جميع العناصر المشكلة للظاهرة أو الظاهرة قيد الدراسة،المجتمع الإحصائي الذي تجرى عليه الدراسة.وعليه فان مجتمع البحث في دراستنا يتمثل في المؤسسات العمومية الجزائرية.

العينة:يعرفها موريس أنجرس أنها مجموعة فرعية من عناصر مجتمع البحث.[1]

وهي جزء من المجتمع الأصلي أو مجموعة فرعية أو جزئية من عناصره ،له خصائص مشتركة وبها يمكن دراسة الكل بدراسة الجزء.[2]

نوع العينة: إن موضوع الدراسة دفعنا لزاماً لاختيار العينة الغرضية (القصدية) :سميت بهذا الاسم لان الباحث يقوم باختيارها طبقا للغرض الذي يستهدف تحقيقه من خلال البحث،ويتم اختيارها على أساس توفر صفات محددة في مفردات العينة تكون هي الصفات التي تتصف بها مفردات المجتمع محل البحث .[3]والمتمثلة الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة ومجوع الموظفين بها.

1_موريس أنجرس وآخرون،منهجية البحث العلمي في العلوم الإنسانية تدريبات عملية،دار القصبة للنشر والتوزيع،ط2006،2004/2،ص294.

2_عيسى يونسي،سامية شينار عائشة عماري،العينة وأسس المعاينة في البحوث الاجتماعية،مجلة الرواق للدراسات الإجتماعية والإنسانية،المجلد 7،العدد2،(2021) ص239_528.

3_وراد زواوي،منهجية إعداد مذكرة تخرج موجهة لطلبة السنة الثانية ماستر،جامعة الجيلالي اليابس سيدي بلعباس ،كلية العلوم الاقتصادية والتجارية وعلوم التسيير،تخصص مالية وتجارة دولية تسويق مصرفي،قسم العلوم التجارية،2021/2020،ص70.

حدود الدراسة:

المجال المكاني:لكل دراسة مرجع مكاني أو إطار أجريت فيه أما بالنسبة لدراستنا فقد أجريت بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

المجال الزماني:أجريت دراستنا بالموسم الجامعي2023_2024 ولقد مرت بمجوعة مراحل:

_من شهر ديسمبر إلى شهر فيفري الاطلاع على موضوع الدراسة وجمع المعلومات حول الأمن المعلوماتي وما تعلق به.

_خلال شهر مارس:بناء إشكالية الدراسة وصياغتها وتحيد أهداف الدراسة وأهميتها.

_خلال شهر أفريل : تحديد منهج الدراسة وأدوات جمع البيانات

_خلال شهر ماي:بناء استمارتي المقابلة والاستبيان والقيام بالدراسة الميدانية وتحليل النتائج.

المجال البشري: المتمثل إقامة مقابلة مع مديرة الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة ،وكذا مع مهندس الإعلام الآلي بالمؤسسة وهو المسئول على المحافظة على الأمن التقني لمعلومات وبيانات المؤسسة،ومقابلة هاتفية مع مدير الوكالة الولائية لتسيير القرض المصغر بغرداية.

وقمنا بمسح شامل للموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة نظرا لقلة عددهم،عن طريق أداة الاستبانة.

9_المقاربة النظرية:

نظرية إدارة نظم المعلومات:

نظم المعلومات: هو أي توليفة (تركيبة) منظمة من الأفرادhuman resources , عتاد الحاسوبcomputer hardware ,برامج الحاسوب computer software, شبكات الاتصالات networksوموارد البيانات data التي يتم جمعها ومعالجتها وتحويلها إلى معلومات وبالتالي توزيعها إلى المستفيدين في المنظمة التي تسمح بالحصولِ، تجميع، تنظيم، معاجلة وتوزيع المعلومات (في شكل نص، صورة، صوت، أو بيانات مرمزة في المؤسسات).[1]

النظرية العامة للنظم:ظهرت نظرية النظم على يد عالم الأحياء النمساوي Ludwig Von) (Bertalanffyعام 7391 والتي أعطاها اسم

(Allgemeine Systemlehre) ثم ترجمت فيما بعد إلى اللغة الانجليزية تحت اسم(General) Systems Theoryأي النظرية العامة للنظم، حيث يمكن القول أن مدخل النظم في الإدارة مشتق أساسا من هذه النظرية بما يناسب علم الإدارة وتطبيقاته في ميدان الأعمال، وتعد هذه النظرية منهجا جديدا يهدف إلى تشكيل مبادئ عامة يمكن تطبيقها على النظم مهما كان نوعها.[2]

المبادئ الأساسية لنظرية النظم العامة:

– النظام : هو الكل المكون من عناصر وأجزاء مترابطة ومتكاملة فيما بينها. فالنظم بصفة عامة تتكون من عناصر متفاعلة ومترابطة فيما بينها. وكل نظام يحتوي على عنصرين كحد أدنى يربط بينهما تفاعل مشترك.

1_مرمي مراد، محاضرات في مقياس :نظم المعلومات، جامعة فرحات عباس سطيف-1 كلية العلوم الاقتصادية والتجارية وعلوم التسيير قسم العلوم الاقتصادية السنة الأولى ماستر تخصص: اقتصاد وتسيير المؤسسات، 2023/2022،ص2.

2_عتيقة بن طاطة،مساهمة نظم المعلومات في عمليات ادارة المعرفة:مقاربة نظرية،كلية العلوم الاقتصادية وعلوم التسيير ،جامعة معسكر،مجلة التنويع الاقتصادية،المجلد04،العدد01،جامعة عين تموشنت_بلحاج بوشعيب،الجزائر،2023،ص33-47.

– النظم الفرعية : يتشكل كل نظام من نظامين فرعيين أو أكثر . فالإنسان نظام يتكون من مجموعة من النظم الفرعية (النظام الهضمي , النظام التنفسي ,....) وكذلك بالنسبة للنظم التعليمية كالجامعة والاجتماعية كالأسرة وغيرها.

– الاتساق : تتصف النظم بالاتساق الداخلي. ويتمثل الاتساق بهيكل النظام نفسه , أي بتجانس بنية مكوناته وأجزاءه. ويظهر هذا الاتساق بوضوح في ظاهرة تكامل الأهداف المنشودة التي يسعى إلى تحقيقها النظام ضمن إطار البيئة التي يعمل في محيطها.

– الكلية والشمولية : النظام ككل واحد ليس مجرد مجموع أجزاءه وعناصره. انه في الواقع نتاج تفاعل الأجزاء والمكونات ولكن ضمن إطار شامل يضم المكونات والأجزاء وينتج منها نظاما يقوم على قاعدة التفاعل والتكامل البيني المتبادل لمكوناته وعناصره أو نظمه الفرعية.

– التكيف : تبادل البيانات والطاقة والمعلومات مع البيئة الداخلية والخارجية (open systems).

أما النظم التي لا ترتبط بعلاقات تفاعل متبادلة مع البيئة فهي لا تستطيع ان تتكيف مع المتغيرات البيئية المحيطة بها وبالتالي تفقد توازنها الداخلي وتفشل في تقديم الاستجابة المناسبة للمتغيرات البيئية (closed systems).[1]

1_علي خاطر محمد،نظم المعلومات الإدارية،جامعة المجمعة.ص12/11
https://m.mu.edu.sa/ar/colleges/college-of-science-and-humanities-rumaah/29378

الإسقاط النظري لنظرية إدارة نظم المعلومات على الدراسة الحالية:

اعتمدنا في دراستنا على نظرية إدارة نظم المعلومات فهي تساعد على فهم كيفية عمل المنظمات وترى بأنها كيان يتكون من نظام موحد يتكون من عدة أنظمة فرعية والمؤسسة محل الدراسة كذالك تمثل النظام العام وفروعها....تشمل الأنظمة الفرعية لهذا النظام ،وان هذا النظام يتأثر بالأنظمة الفرعية الأخرى، وهذه النظرية تنظمن تحليل الهيكل التنظيمي والمعلومات والية التخطيط والتحكم،وهذا ما نقوم به في دراستنا،إن إستراتيجية الأمن المعلوماتي تمثل النظام الذي تسعى الأنظمة الفرعية لحمايته والمحافظة عليه،ساعدتنا هذه النظرية في فهم عناصر المشكلة المتمثلة في الإستراتيجية الأمنية وعلاقتها مع عناصر البيئة الخارجية لان هذه النظرية تنظر للنظام الإداري كنظام فرعي من النظام الاجتماعي العام يتفاعل معه ويتأثر به بشكل مستمر وهذا ينطبق على دراستنا فالمعلومات هي أساسا من إنتاج الإنسان أو نستطيع القول من إنتاج الفاعلين في المؤسسة فهم من يقومون بإمداد المنظمة بالمدخلات الضرورية وهم يشكلون أيضا جزء من هذه المعلومات ويؤثرون على امن هذه المعلومات بتوفير بحمايتها أو المساعدة على اختراقها،

تؤكد هذه النظرية بأهمية التخطيط والتنظيم والتوجيه والرقابة في العملية الإدارية وفي دراستنا هذه نحاول معرفة ماذا كانت المؤسسة محل الدراسة تقوم بهذا أو لا.

تطرقت هذه النظرية أيضا لضرورة امن المعلومات في المنظمات وعن عناصر امن المعلومات وعن المتطلبات الفنية والإدارية لأمن الأنظمة والمتمثلة في إستراتيجية امن المعلومات وأهدافها وبإسقاطها على الدراسة الحالية نجد ضرورة وجود إستراتيجية امن معلوماتي بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

الفصل الثاني :الجانب الميداني للدراسة

_**المبحث الأول**:إجراءات الدراسة الميدانية

_ **المبحث الثاني**: عرض وتفسير البيانات الخاصة بالمقابلة.

_**المبحث الثالث**:عرض وتفسير البيانات الخاصة بالاستبيان

_**المبحث الرابع**:الاستنتاجات العامة للدراسة.

المبحث الأول:إجراءات الدراسة ميدانيا

التعريف بالوكالة الوطنية لتسيير القرض المصغر:

لمحة تاريخية

اعتمدت الجزائر القرض المصغر بمثابة أداة لمحاربة الهشاشة حيث تسمح لفئة الأشخاص المحرومين من تحسين ظروفهم المعيشية وهذا من خلال استحداث أنشطتهم الخاصة التي تمكنهم من الحصول على المداخيل .

بحيث ظهر القرض المصغر لأول مرة في الجزائر سنة 1999 ميلادي إلا انه لم يعرف (في صيغته السابقة) النجاح الذي كانت تتوخاه السلطات العمومية بسبب ضعف المرافق أثناء مراحل إنضاج المشاريع ومتابعة انجازها .

وقد تبين ذلك خلال الملتقى الدولي الذي نظم في ديسمبر 2002 حول موضوع (تجربة القرض المصغر في الجزائر) وبناءا على التوصيات المقدمة خلال هذا التجمع الذي ضم عدد معتبر من خبراء في مجال التمويل المصغر بحيث تم إنشاء الوكالة الوطنية لتسيير القرض المصغر بموجب المرسوم التنفيذي رقم 04/14 المؤرخ في 22 جانفي 2004 .

إطار نشأة الوكالة الوطنية لتسيير القرض المصغر:

الإطار العام للوكالة الوطنية لتسيير القرض المصغر

يندرج برنامج القرض المصغر في إطار التنمية الاجتماعية المستهدفة من طرف السلطات العمومية والتي تهتم بترقية قدرات الأفراد والفئات السكانية للتكفل بذاتهم لبلوغ مستوى معيشي نزيه ومنصب شغل معتبر بتطبيق سياسة اجتماعية جديدة هدفها الأساسي تخفيض الكفلة الاجتماعية من اجل الانتقال لاقتصاد السوق.

بهذا المعنى هي سياسة دعم مباشر مستهدف وتساهمي تقترح كبديل للروح الاتكالية في هدا الإطار تم تجسيد مشروع إنشاء الوكالة الوطنية لتسيير القرض المصغر.

الإطار القانوني والتشريعي

عقب التوصيات المنبثقة عن الملتقى الدولي خلال ديسمبر عام2002م التجربة الجزائرية في القرض المصغر تم إنشاء الوكالة الوطنية لتسيير القرض المصغر بموجب:

_المرسوم الرئاسي رقم11/133 المؤرخ في 22 مارس 2011 المتعلق بجهاز القروض المصغرة
_المرسوم التنفيذي رقم04/14 من22 جانفي 2004م المتعلق بإنشاء والمحدد لهيكل صندوق الضمان المشترك القروض المصغرة.
_المرسوم التنفيذي رقم134/11 من 22 مارس2011 والمعدل للمرسوم التنفيذي رقم15/04 من22جانفي2004 الذي يحدد شروط ومستوى الإعانات الممنوحة للمستفيدين من القروض المصغرة
_المرسوم التنفيذي رقم 16/04 من22 جانفي 2004 المتعلق بإنشاء وتحديد هيكل صندوق الضمان المشترك القروض المصغرة

تعريف الوكالة الوطنية لتسييرالقرض المصغرANGEN:

تعبر الوكالة الوطنية لتسيير القرض المصغر من أهم هياكل دعم وتعزيز المؤسسات الصغيرة والمتوسطة في الجزائر حيث تهدف إلى منح قروض مصغرة إلى الشباب الراغب في إنشاء مشروع مصغر بالإضافة إلى تغطية القروض التي منحها البنك وذلك بهدف تشجيع هذه الأخيرة على منح الائتمان لتمويل عملية إنشاء المؤسسات المصغرة.

تعريف القرض المصغر

هو عبارة عن قرض يمنح لفئة المواطنين الذين هم من دون مدخول أو لديهم مدخول غير منتظم مخصصا لخلق نشاطات جديدة بما في ذلك الأنشطة الممارسة منزليا قصد شراء المعدات للشروع في العمل.

مهام وأهداف المؤسسة

أولا: أهداف المؤسسة

للوكالة الوطنية لتسيير القرض أهمية بالغة إذ تساهم في مكافحة البطالة والفقر في المناطق الحضرية والريفية من خلال تشجيع العمل الحر والعمل في البيت والحرف والمهن ولاسيما والفئات النسوية ومنه تتخلص مهام الإدارة فيما يلي:

- تسيير جهاز القرض المصغر وفقا للقوانين المعمول بها.
- دعم وتوجيه ومرافقة المستفيدين في تجسيد أنشطتهم لاسيما فيما يتعلق بتمويل مشاريعهم.
- إبلاغ المستفيدين الذين أهلت مشاريعهم في الجهاز بمختلف الإعانات الممنوحة والعقود المتعلقة بالوكالة ومساعدتهم لدى المؤسسات والهيئات المتعلقة بتجسيد مشاريعهم بما في ذلك الشركاء الماليون للبرنامج.
- الحفاظ على العلاقة المستمرة مع البنوك والمؤسسات المالية فيما يخص تمويل المشاريع وتنفيذ مخطط التمويل وتتابع واستغلال ديون المستحقة في الوقت المحدد.
- تكوين حاملي المشاريع والمستفيدين من القروض المصغرة فيما يخص تقنيات تمويل وتسيير الأنشطة المدرة المداخيل
- تنظيم المعارض معرض بيع جهوية وطنية لمنحات القرض المصغر.
- تكوين مستمر للموظفين المسؤولين عن تسيير الجهاز.

ثانيا: أهداف المؤسسة

من خلال إنشاء الوكالة الوطنية لتسيير المصغر هناك مجموعة من الأهداف التي سطرت وهي:

_تنمية روح المقاولاتية تنحل محل الاتكالية وبالتالي تساعد على الإدماج الاجتماعي والتنمية الفردية للأشخاص

_دعم وتوجيه ومرافقة المستفيدين في تنفيذ أنشطتهم لاسيما فيما يتعلق بتمويل مشاريعهم ومرحلة الاستغلال.

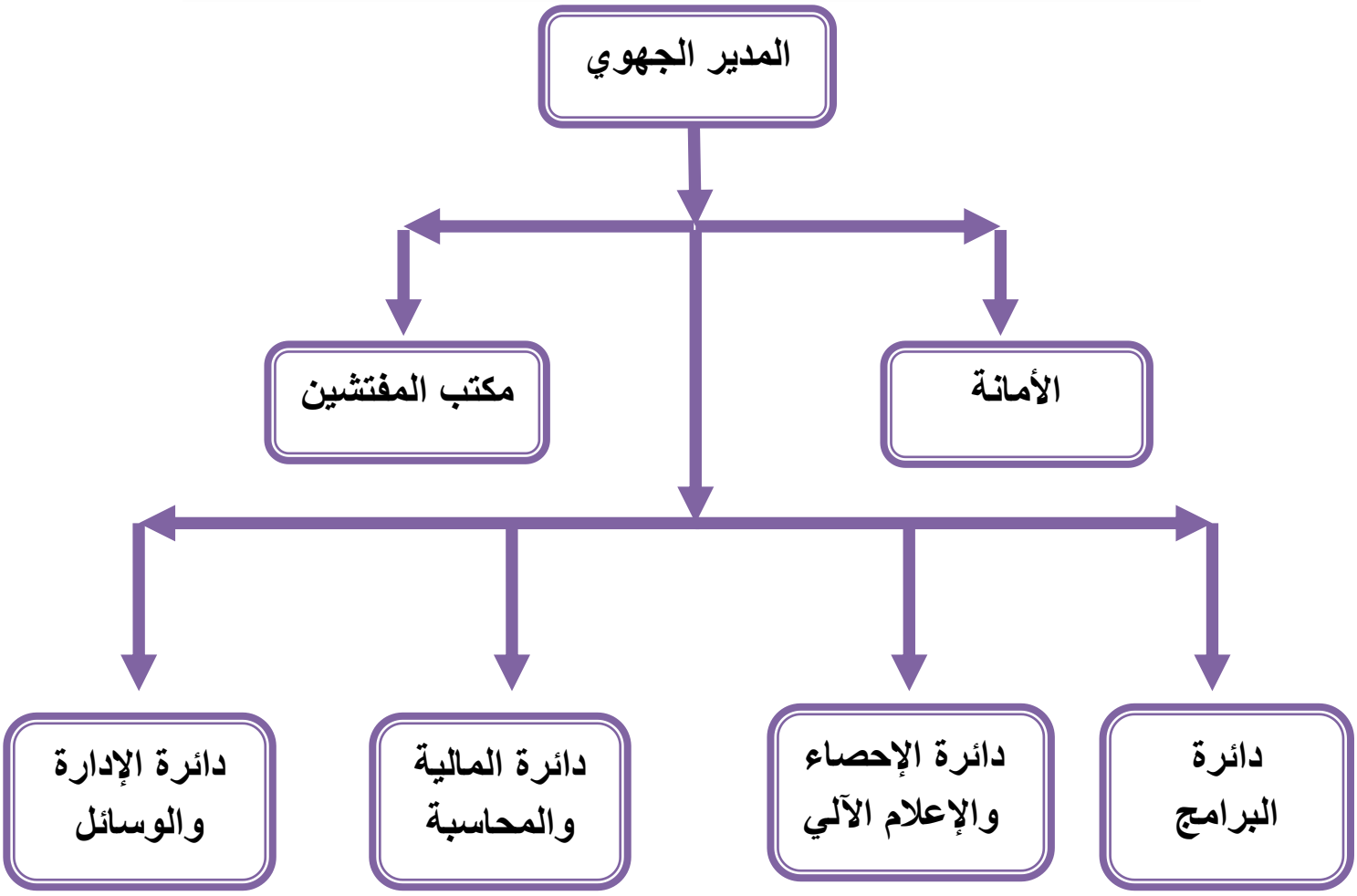
_متابعة الأنشطة المنجزة من طرف المستفيدين مع الحرص على احترام اتفاقيات والعقود التي تربطهم مع الوكالة الوطنية لتسيير القرض

_تكوين حاملي المشاريع والمستفيدين من القرض المصغرة في مجال تقنيات تمويل وتسيير الأنشطة المدرة لمدا خيل والمشاريع جد المصغرة

دعم تسويق منتجات القروض المصغرة عن طريق تنظيم المعارض عرض/بيع

_اخذت المعلومات من الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة2024/05/19

الهيكل التنظيمي للوكالة الوطنية للقروض المصغرة الفرع الجهوي ورقلة



الهيكل التنظيمي للمؤسسة:من إعداد الطالبة بالاعتماد على المقابلة.

المبحث الثاني: عرض وتفسير البيانات الخاصة بالمقابلة.

المحور الأول: الإجراءات و الوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية معلوماتها

1/أساليب الحماية المادية.

_الحماية المادية للمؤسسة من خلال إحكام السيطرة والرقابة على مداخل الوكالة للوصول إلى القدر الممكن من امن المعلومات من خلال اتخاذ إجراءات شاملة ضد الأخطاء عن طريق تحيد حركة الدخول والخروج ليلا ونهارا ،وذلك بتسخير العنصر البشري داخل المؤسسة المتمثل في أعوان الأمن الذين يعملون بالتناوب ودون توقف ليلا ونهارا وهذا الذي يعتبر عنصر أساسي للمحافظة على الأمن المادي للمؤسسة ككل المتمثل في (مقر المؤسسة،التجهيزات ،العتاد،الأفراد) .

_تتوفر المؤسسة على مجموعة من المكاتب وكل مكتب يتم حمايته بقفل يحصل على مفتاحه صاحب المكتب فقط.

_تخصيص أماكن لحماية وحفظ المعلومات والبيانات التي تتوفر عليها المؤسسة(السجلات،العتاد،أجهزة الإعلام الآلي،آلات النسخ،الخواتيم)وحمايتها من المخاطر الطبيعية مثل الحرائق عن طريق توفير مطافئ الحماية،أو مخاطر أخرى من خلال عمل نسخ احتياطية.

_لا تتوفر المؤسسة على كاميرات التصوير التليفزيونية التي يمكن التحكم فيها وهذا يمكن أن يؤثر بشكل سلبي على امن المؤسسة كون هذه الكاميرات تراقب مداخل المؤسسة ومداخل غرف النظام وتتوفر على جهاز إنذار ينبه عند حدوث أي خطر.

2/أساليب الحماية البرمجية

1)برامج مكافحة الفيروسات:

_تقوم المؤسسة بشراء البرامج المضادة الفيروسات لمنع واكتشاف فيروسات الحاسوب والديدان وأحصنة طروادة وبرامج التجسس وغيرها من البرمجيات الخبيثة للمحافظة على بيانات المؤسسة من خطر الاختراق.

2)تشفير البيانات :

_هي تقنية تلجا المؤسسة إليها لتشفير قاعدة بياناتها ، إذا تم نقل هاته المعلومات الحساسة عبر الشبكات ، وتحويل المعلومات إلى رموز ونصوص مشفرة لا يمكن قراءتها سوى مهندس الإعلام الآلي بالمؤسسة وذلك من اجل منع الوصول الغير مصرح به.

3)امن الشبكة:

_تشفير شبكة (wifi) عن طريق العنوان الفيزيائي:لا يمكن لأي شخص الدخول لشبكة (الويفي) الخاصة بالمؤسسة سواء كان من المواطنين أو الموظفين حتى إذا كان يملك كلمة المرور إذا لم يسمح له مهندس الإعلام الآلي.

4)التوثيق متعدد البرامج :

_من اجل الوصول إلى الحساب أو النظام في المؤسسة يجب على المستخدم تقديم أشكال متعددة من تحديد الهوية(اسم المستخدم وكلمة المرور).

5)النسخ الاحتياطية:

_تقوم المؤسسة بعمل نسخ شهرية للبيانات في قرص صلب خارجي يخبأ في مكتب الإعلام الآلي للتأكد من حماية المعلومات من التلف في حال حدوث حريق أو وصول الماء إلى تلك المعلومات.

6)تصحيح البرامج :

_ تعمل المديرية العامة الوكالة الوطنية لتسيير للقرض المصغر (المتواجدة بالعاصمة) على إرسال التحديثات في تطبيقات البرامج لمعالجة نقاط الضعف وإصلاح الأخطاء وإضافة ميزات جديدة في البرامج القديمة التي تكون أكثر عرضة للهجمات الالكترونية عند اكتشاف أي خطا من طرف مهندس الإعلام الآلي في برامج الأمن في المؤسسة يتم تبليغ المديرية العامة وهي بدورها تعمل على استحداث تحديثات لبرامج الأمن والحماية .

7)توفير مصدر احتياطي للطاقة الكهربائية:

_تتوفر المؤسسة على مخزن للطاقة في حال حدوث خلل كهربائي.

8)الأمن السحابي:

_لا تلجأ المؤسسة لبرنامج الأمن السحابي لان المعلومات تخزن عند شركات الأمن السحابي مثل (dropbox ,google, ...) وهذا في حد ذاته قد يشكل خطر على الأمن المعلوماتي للمؤسسة إذا حدث خلل في هاته الشركات الخاصة بالأمن .

_لهذا تتوفر المؤسسة خادم خاص (ftp) خاص بالمديرية العامة (الوكالة الوطنية لتسيير للقرض المصغر المتواجدة بالعاصمة)تقوم مختلف الوكالات الفرعية التبعة لها بالتخزين فيه وهذا ما يوفر أمان أكثر للبيانات والمعلومات الخاصة بالمؤسسة.

3/أساليب الحماية التنظيمية والإدارية.

1_**تصنيف المعلومات:**تختلف درجة حماية المعلومات باختلاف سريتها وأهميتها في المؤسسة فهناك:

_معلومات لا تحتاج إلى حماية مطلقا ويحصل عليها من يريد ومتى يشاء وهي المعلومات العامة التي تصل إلى المواطنين

_بيانات تحتاج إلى نسبة معينة من الحماية يمكن لأشخاص معينين أن يحصلوا عليها وهي البيانات المتعلقة القوائم والملفات المتعلقة بالمواطنين المتعاملين مع الوكالة.أو البيانات والمعلومات التي تتعلق بالموظفين بالمؤسسة

_بيانات تتطلب حماية قصوى ولا تتوفر إلا لدى المدير أو مصلحة معينة

2_**التوعية داخل المؤسسة:**

لا يمكن توفر الأمن المعلوماتي داخل المؤسسة من دون وعي بموضوع الأمن المعلوماتي وخطورته لدى الموظفين وتعمل المؤسسة بشكل جدي وصارم في هذا الموضوع من خلال القيام بعمليات تحسيسية مباشرة وتضييق رقعة تداول المعلومة .

3_**وضع سياسة لآمن المعلومات بالمؤسسة:**

وهي جملة القواعد والقوانين التي تنظم عمل المؤسسة لتحقيق الأمن المعلوماتي

تمثلت في:

1/أمن المعلومات المهنية و الشخصية :

الهدف : تحفيز المستخدمين لحماية معلوماتهم المهنية و الشخصية:

1. يمنع الحفاظ على المعلومات السرية الخاصة باسم المستخدم و كلمة المرور وكذا رمز PIN, على دعائم ورقية أو الكترونية.
2. يجب أن يكون حجم كلمة المرور أكبر من ثمانية (08) أحرف .
3. يجب أن تتكون كلمة المرور من الأحرف الأبجدية الرقمية و الحروف (كبيرة و صغيرة) وكذا الرموز الخاصة .
4. يجب أن لا تكون كلمة المرور سهلة المنال (كالاسم و اللقب وأرقام الهواتف و تواريخ أعياد الميلاد .....)
5. عدم استخدام الكلمات الشائعة (Qwerty.Azerty...).
6. يجب تغيير كلمات المرور عند تسجيل الدخول الأول إذا قدم من قبل الآخرين.
7. يجب تغيير المعلومات السرية بشكل دوري .
8. يجب عدم تبادل معلومات المصادقة السرية .
9. يجب أن لا تستخدم نفس المعلومات السرية على حسابات متعددة .
10. يجب السماح لمستخدمي الشبكة المعلوماتية الولوج إلا للموارد المسموح بها, علما أن هناك عقوبات تطبق في حالة محاولة اختراق الشبكة المعلوماتية الداخلية من طرف مستخدميها .
11. يتم الحفاظ على كلمات المرور للمستخدمين الذين غادرو الوزارة أو مصالح الغير مركزية و ذلك لمدة (01) سنة واحدة, ثم يتم حذفها نهائيا.

2/ التدابير التي يجب اتخاذها عند أداء مهمة إلى الخارج:

الهدف: توعية الإطارات المكلفة بأداء مهام إلى الخارج بالمخاطر الالكترونية التي يمكن أن تتعرض إليها معلومات الشخصية وكذا المهنية.

وعليه يجب تنفيذ التدابير الآتية :

1. يمنع استخدام الأجهزة الالكترونية أو اللوحات الالكترونية العامة أو المشتركة قصد الوصول إلى حساب البريد الالكتروني المهني أو التطبيقات المهنية.

2. يمنع ترك الأجهزة الالكترونية أو اللوحات الالكترونية المهنية لاسيما دعائم التخزين في متناول الأشخاص الأجانب و الحفاظ عليها.
3. يجب تشغيل وسائل الاتصال بدون الكوابل مثل (Wi-Fi / bluetooth)' إلا عند الضرورة وتوقيف تشغيلها عند الانتهاء منها .
4. يجب حذف كافة البيانات المهنية الحساسة غير الضرورية لأداء المهمة من جميع الدعائم الالكترونية وذلك قبل السفر على الخارج.
5. يجب تبليغ الإدارة المركزية و الممثل الدبلوماسي الجزائري في حالة أي عملية تفتيش آو مصادر لأجهزة الإعلام الآلي من قبل السلطات الأجنبية .
6. يمنع استخدام الأجهزة الالكترونية المهداة أثناء أداء المهمة في الخارج لأغراض مهنية.
7. يجب ذكر في التقارير قائمة الأجهزة الالكترونية المهداة والتي تم تشغيلها أثناء أداء المهمة .
8. يجب استعمال البريد الالكتروني المهني بطريقة حصرية لتبادل المعلومات و الوثائق مع الأجانب ويمنع منعا باتا تبادل المعلومات و الوثائق معهم في شكل دعائم الكترونية.
9. يجب على المكلف بالمهمة إلى الخارج تغيير كلمات المرور المستخدمة خلال أداء المهمة.

3/ نقل البيانات:

الهدف : حماية البيانات و المعلومات المنقولة في الشبكة المعلوماتية وذلك قصد ضمان حمايتها و سريتها.

1. يلزم السهر على السير الحين لتبادل و تحويل المعطيات الالكترونية مع الإدارات و المؤسسات وذلك قصد ضمان متطلبات الأمن (السرية , النزاهة .....) أثناء عملية التحويل .
2. لا يمكن تبادل المعلومات و البيانات إلا برخصة من المسئول المباشر.

3. يجب وضع ضوابط وإجراءات تقنية لضمان تبادل المعلومات و البيانات.

4/ البريد الالكتروني و الاتصال عبر الانترنت:

الهدف: التحكم في استعمال الانترنت على مستوى الإدارة أو المؤسسات و ضمان حماية أنظمة الإعلام من الهجمات الالكترونية.

وعليه لا يمكن استخدام البريد الالكتروني المهني و الموضوع من طرف الإدارة تحت تصرف المستخدمين إلا لأغراض مهنية و تحقيقا لهذه الغاية , **يمنع منعا باتا**, مايلي:

1. إرسال رسالة خاصة أو شخصية من خلال البريد الالكتروني المهني.
2. استخدام عنوان البريد الالكتروني للتسجيل في الشبكات الاجتماعية مثل facebook و المنتديات ومواقع الانترنت.
3. استخدام عناوين البريد الالكتروني الشخصية لإرسال الوثائق المهنية.
4. فتح البريد الالكتروني المهني في الأماكن العامة كمقهى الانترنت.
5. فتح المرفقات أو الوصلات المرسلة كعناوين البريد الالكتروني غير المعروفة, وكذا الحذر عند استخدام البريد الالكتروني وذلك من خلال ضمان ما يلي :

- ✓ التحقق من عنوان المرسل إليه .
- ✓ يحق للمرسل إليه التطلع على محتوى النص المرسل.
- ✓ التأكد من الوثائق المرفقة مع الإرسال.

5/استخدام الانترنت لأغراض مهنية:

يجب على الموظفين المستغلين لشبكة الانترنت على مستوى الإدارة أو المؤسسات التعهد بالتقيد وتنفيذ التعليمات التالية:

1.عدم استخدام الانترنت لأغراض خبيثة أو فاحشة أو احتيالية أو حادقة أو تشهيرية أو إباحية أو غير قانونية

1. عدم محاولة استغلال الشبكة المعلوماتية للولوج إلى أي جهاز كمبيوتر أو حساب الكتروني دون رخصة دخول ;
2. عدم تحميل الملفات , إلا بعد التأكد من مسحها من جميع الفيروسات.
3. عدم تحميل فيديوهات أو صور دون دواعي مهنية, قصد الحفاظ على تدفق العالي للانترنت في الشبكة المعلوماتية الداخلية.
4. احترام حقوق التأليف للبرمجيات.

5/قواعد استخدام وسائل التواصل الاجتماعي:

1. قواعد استخدام وسائل التواصل الاجتماعي على المستوى المهني:

في حالة اعتماد الإدارة أو المؤسسة استغلال التواصل الاجتماعي لاستخدام مهني فلا بد من تنفيذ التعليمات التالية:

أ- إعداد دليل استخدام للأشخاص المكلفين بتسيير و متابعة مواقع التواصل الاجتماعي التي تديرها الوزارة أو المصالح المركزية أو المصالح الواقعة تحت الوصاية .

ب- الحرص على منع القرصنة و الدخول غير المصرح به إلى حسابات مواقع التواصل الاجتماعي المصالح اللامركزية أو المصالح الواقعة تحت الوصاية,

بالاظافة إلى ذلك فان الموظفين المسؤولين عن هذه الحسابات يجب عليهم التقيد بما يلي :

- استخدام حسابات وكلمات مرور مختلفة لكل شبكة تواصل الاجتماعي
- يجب أن تستوفي كلمات المرور معايير محددة أعلاه.

2- قواعد استخدام وسائل التواصل الاجتماعي على المستوى الشخصي :

بالنسبة للاستخدام الخاص لوسائل التواصل الاجتماعي فعلى الإدارة الالتزام بـ:

أ- منع استخدام عنوان البريد الالكتروني المهني لفتح حسابات وسائل التواصل الاجتماعي.

ب- منع نشر البيانات ذات الصلة بالوظيفة , الرتبة أو المسؤولية على الشبكات الاجتماعية.

ج–منع الكشف عن أي معلومات تتعلق بالحياة المهنية على الشبكات الاجتماعية

د– تحسيس مستخدمي الشبكات الاجتماعية بمخاطر الكشف عن البيانات الخاصة أو الشخصية.

6/ تامين الاتصال

الهدف: حماية و تامين المعلومات و البيانات السرية

1. يمنع منعا باتا إرسال معلومات سرية عن طريق خط هاتفي غير مؤمن.
2. يجب وضع التدابير الأمنية الأساسية عند تبادل المعطيات السرية عن طريق البريد الالكتروني
3. يجب وضع التدابير الأمنية الأساسية عند تبادل المعطيات السرية عن طريق بروتوكول الانترنت (ip) .
4. يمنع منعا باتا تبادل المعلومات السرية عن طريق الأرضيات الالكترونية الموطنة في الخارج.
5. يجب أن تكون جميع البيانات و المعلومات السرية مشفرة عند إرسالها عبر الشبكات المعلوماتية العمومية والغير مستعملة لخطوط خاصة.

7/ الشبكة المعلوماتية بدون كوابل

الهدف: حماية الشبكة المعلوماتية من التصنت أو الولوج الغير مرخص.

وعليه , يجب التقيد و تنفيذ التعليمات التالية:

1. يجب وضع نقاط الوصول للشبكة المعلوماتية من دون كوابل في أماكن محمية تحت المراقبة و الوصول إليها محدود.

2. يجب الحرص على أن محيط وصول تدفق الشبكة يكون محصور على مستوى الإدارة أو المؤسسة وذلك عن طريق دراسة وتحديد أماكن وضع نقاط الوصول للشبكة المعلوماتية من دون كوابل.
3. عدم فتح الشبكة للجميع وتحديد الولوج إليها عن طريق استغلال كلمة المرور مركبة.
4. تكون كلمة المرور مشفرة عند تسليمها للمستخدمين المرخص لهم لاستغلالها

8/ اقتناء و وضع البرمجيات

الهدف: الحد من الخطر المتعلق بأمن أنظمة الإعلام عند اقتناء و وضع برمجيات. وعليه يجب التقيد وتنفيذ التعليمات التالية:

1. يمنع اقتناء أو استعمال البرامج المقرصنة وكل البرامج والأنظمة المكتسبة يجب أن تكون لها ترخيصات رسمية.
2. يمنع تحميل البرمجيات عن طريق الانترنت من خلال المواقع غير الرسمية للمحرر
3. يمنع اقتناء برمجيات أو التطبيقات التي أعلن الناشر نهاية دعمها.
4. من المستحسن الحصول على احدث نسخة من الأنظمة و البرمجيات.
5. يمنع على المستخدم النهائي من تثبيت برمجيات أو تطبيقات على جهاز الكمبيوتر المهني الخاص به وفي حالة الضرورة يجب طلب موافقة مسبقة من الهيكل المسؤول عن حماية أنظمة الإعلام على مستوى الوزارة أو الهياكل اللامركزية.
6. لا يثبت على جهاز الكمبيوتر المهني إلا نظام الاستغلال و البرمجيات الضرورية لمهام الوزارة أو المصالح اللامركزية أو المصالح الواقعة تحت الوصاية.

7. ينبغي الإبلاغ عن الأخطاء و الأعطاب عند وقوعها للهيكل المكلف بصيانة الأجهزة الالكترونية خاصة منها الكمبيوتر على مستوى الوزارة أو المصالح اللامركزية أو المصالح الواقعة تحت الوصاية
8. يجب الحرص على تحين البرمجيات و الأنظمة المستعملة.

9/العمليات التي يقوم بها المستخدم:

1. تفعيل خاصية التوقيف المؤقت لأجهزة الكمبيوتر.
2. إعلام المديرية المكلفة بحماية أنظمة الإعلام في حالة اكتشاف جهاز جديد متصل بجهاز العمل عن طريق الشبكة المعلوماتية الداخلية
3. إعلام المديرية المكلفة بحماية أنظمة الإعلام في حالة غياب برنامج الحماية عن جهاز الكمبيوتر المهني أو في حالة ظهور خروقات.
4. يمنع إيصال الأجهزة الالكترونية الشخصية إلى جهاز الكمبيوتر المهني.
5. مسح جميع دعائم الالكترونية قبل استخدامها على جهاز الكمبيوتر المهني
6. إيقاف تشغيل جهاز الكمبيوتر المهني خلال فترات عدم النشاط (ليلا – عطلة–نهاية الأسبوع) .
7. يمنع منعا باتا تناول المشروبات أو التدخين بالقرب من وسائل معالجة المعلومات

10/ استخدام جهاز الهاتف النقال و وسائط التخزين:

<u>الهدف:</u> تجنب ضياع أو سرقة المعلومات المخزنة في الهواتف النقالة. وعليه , يجب التقيد وتنفيذ التعليمات التالية:

1. يجب على المستخدم حفظ بحوزته أجهزته النقالة الخاصة كالهاتف و وسائل التخزين الالكترونية وذلك خلال تنقلاته المهنية.
2. يجب إبلاغ السلم الإداري , مباشرتا عن فقدان أو سرقة الجهاز المحمول المهني.

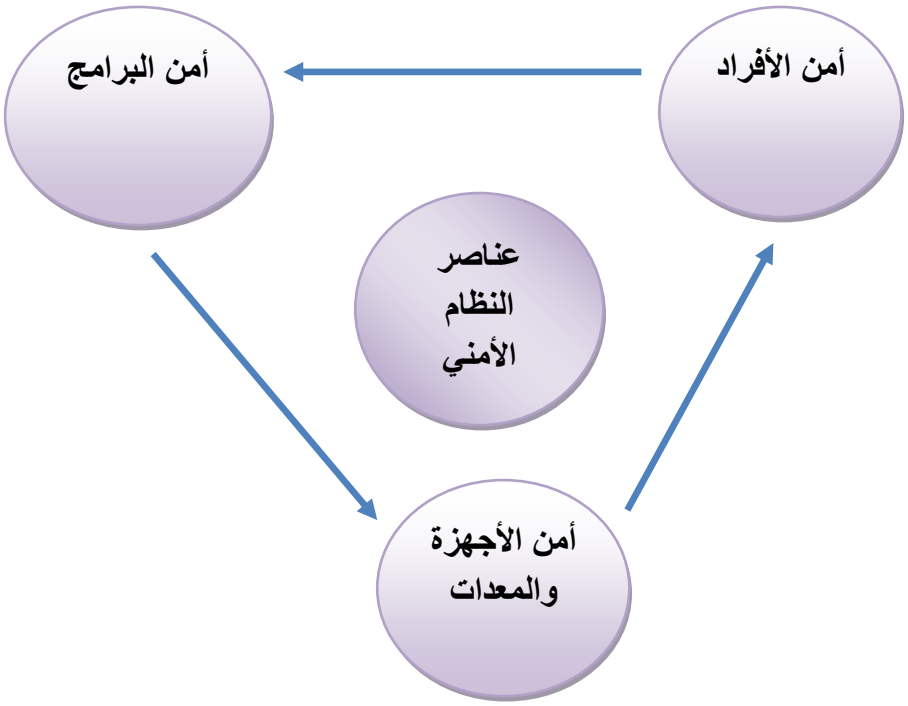
3. يمنع على أي شخص من خارج الوزارة آو المصالح اللامركزية أو المصالح الواقعة تحت الوصاية نقل الوثائق على دعائم الالكترونية أو تبادلها عن طريق البريد الالكتروني.
4. يجب مسح البيانات التي تتطلب استخدام دعائم الالكترونية وذلك قبل استعمالها

11/ إدارة البيانات

1. يجب تامين سرية و سلامة البيانات الحساسة عن طريق ضمانات من الوسائل التقنية المناسبة بما في ذلك التشفير .
2. الحرص على حفظ الوثائق الحساسة المطبوعة و المستنسخة ومنع استخدام آلات التصوير وأجهزة الاستنساخ الأخرى.

12/ حفظ البيانات

1. يمنع منعا باتا تخزين البيانات المهنية على منصات التوطين خارج البلاد Plate forme hebergée مثل (Google drive)
1. يتم الحفظ الاحتياطي على دعم خارجي مخصص.
2. يجب أن يتم تنفيذ عمليات الحفظ الاحتياطي وفقا للقواعد محددة من المديرية المكلفة بأنظمة الإعلام .



عناصر النظام الأمني:من إعداد الطالبة.

المحور الثاني:الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهري ورقلة.

1_من خلال تحليل المقابلات التي قمنا بها توصلنا إلى أن مهمة حماية البيانات هي مسئولية كل دوائر المؤسسة من المدير حتى أعوان الأمن .

2_ تنسب مهمة حماية المعلومات والبيانات الحساسة في المؤسسة بالدرجة الأولى إلى المستويات الإدارية العليا المتمثلة في الدائرة المكلفة بالإحصاء والإعلام الآلي يشرف على هذه الدائرة مهندس إحصاء، ومهندس إعلام ألي مهمته المحافظة على الأمن المعلوماتي للمؤسسة من خلال: المحافظة على سرية البيانات والمعلومات وسلامتها من التغيير أو التعديل فيها واستمرارية توفرها في حال ما احتاجت المؤسسة الوصول إليها من خلال توفير برامج الأمن وأساليب الحماية وكذالك مراقبة قاعدة المعطيات (يتم فيها تسجيل المستفيدين من منح القروض ويتم فيها تسجيل القروض التي قام المستفيدين إرجاعها بعد نجاح مشاريعهم). هذا يتوافق مع النتائج التي توصلت إليها دراسة (امال بن اعراب ،الخطر المعلوماتي ومسؤولية حماية المعلومة في المؤسسة الاقتصادية،2021).

3_لكل دائرة في المؤسسة معلومات وبيانات خاصة بها لا يمكن لأي دائرة التصريح ببياناتها لدائرة أخرى، يحمي مهندس الإعلام الآلي هاته البيانات عن بعد بأنظمة الحماية دون أن يعرف ماهيتها.

4_تختلف أشكال المعلومات و سريتها حسب الجهات الموجودة بالمؤسسة:

_الأمانة: المراسلات المتعلقة بالمؤسسة(البريد الصادر والوارد) .

_المفتشين:مهمتهم إجراء التقارير حول المواطنين أصحاب المشاريع المستفيدين من القروض .

_دائرة الإحصاء والإعلام الآلي: Département etude statistique et informatique:القيام بالإحصاءات ومهندس الإعلام الآلي يقوم بتوفير الوسائل اللازمة لحماية مختلف بيانات ومعلومات المؤسسة.

_دائرة البرامج (Département Dévelopement Programme): تقوم بتجميع ملفات طلب أصحاب المشاريع للحصول على القرض.

_دائرة المحاسبة والمالية department finance et comptabilité : حساب الأموال التي تقدمها الشركة لأصحاب المشاريع ،والحسابات المتعلقة بالمعاملات والأموال .

_دائرة الإدارة والوسائل: department administration et moyens تملك الملفات الخاصة بالموظفين ،وتوفير حاجيات المؤسسة من عتاد ومستلزمات.

كل جهة تحتفظ بسرية معلوماتها الخاصة ولا تصرح بها إلى جهة أخرى ماعدى مدير المؤسسة.

المحور الثالث: البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها.

تعتبر المعلومة موردا رئيسيا وأساسيا في المؤسسة وجب حمايتها لان فقدانها أو تغيرها يترتب عليه عواقب وخيمة وتختلف درجة حماية المعلومات بالمؤسسة حسب سريتها وأهميتها وهي كالتالي:

1_معلومات لا تحتاج إلى حماية مطلقا ويحصل عليها من يريد ومتى يشاء وهي المعلومات العامة التي تصل إلى المواطنين مثل (معلومات حول القرض المصغر وماهيته، الشروط اللازمة للحصول على القرض،المبالغ التي يستطيع المتعامل الحصول عليها ،الشروط التي يجب أن تتوفر في صاحب الملف، عند توفر مناصب الشغل في المؤسسة تقوم بالتصريح بالشروط التي يجب أن تتوفر في صاحب المنصب)

2_بيانات تحتاج إلى نسبة معينة من الحماية يمكن لأشخاص معينين أن يحصلو عليها وهي البيانات المتعلقة القوائم والملفات المتعلقة بالمواطنين المتعاملين مع الوكالة. أو البيانات والمعلومات التي تتعلق بالموظفين بالمؤسسة مثل(البيانات الشخصية المتعلقة بالموظفين،الرواتب،العقوبات،الخصم،النظام الداخلي للمؤسسة)

وكما ذكرنا سابقا أن لكل دائرة في المؤسسة معلومات وبيانات خاصرة بها ،لا يمكن لأي دائرة التصريح ببياناتها لدائرة أخرى ومعلومات كل الدوائر المدير على دراية بها.

3_بيانات تتطلب حماية قصوى ولا تتوفر إلا لدى المدير أو مصلحة معينة وهي المعلومات السرية المتمثلة في الإستراتيجية العامة للمؤسسة والمشاريع والخطط المستقبلية(توجد لجان خاصة تختارهم المديرية العامة لتطوير مشاريع مستقبلية لا تتوفر معلومات هذه المشاريع إلا لدى المديرية العامة في الجزائر ومديرة الوكالة)

المحور الرابع: المخاطر التي تهدد امن المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

1_المخاطر الطبيعية: هذه المخاطر تخرج عن نطاق سيطرة المؤسسة وهي مختلف الكوارث الطبيعية مثل(الحرائق،والفيضانات،الزلازل) التي تعتبر تهديدا حقيقيا للأجهزة المادية للمؤسسة وإتلاف نظام المؤسسة كليا أو إلحاق الضرر به ،بينما أعمال التخريب والسرقة تقوم المؤسسة بإجراء جملة من التدابير الوقائية والإجراءات لتجنب الوقوع فيها من خلال تزويد المؤسسة بأعوان الأمن الذين يعملون بالتناوب ولا تترك المؤسسة من دون حراسة بتاتا.

2_المخاطر التقنية:

_تعتبر البرمجيات الخبيثة المختلفة(كالفيروسات،أحصنة طروادة،...)هي أكثر التهديدات التي تلحق أضرارا بأجهزة ومعلومات المؤسسة،وهذا ما يدفع المؤسسة لشراء التحديثات في برامج مكافحة البرامج الخبيثة ،كذالك ستلجأ المؤسسة في المستقبل القريب للجوء للجدران النارية ...

3_قلة وعي الموظفين:

_أكثر خطر يواجه المؤسسة هو (مواقع التواصل الاجتماعي)فقد يلجا موظفي المؤسسة عند حدوث أي مناوشات يقوم الموظف بنشر معلومات عن المؤسسة في هذه المواقع وهذا يعتبر من أشكال اختراق سرية الأمن المعلوماتي للمؤسسة

_جهل وقلة وعي عمال المؤسسة بالبرامج التي قد يثبتونها في الأجهزة المعلوماتية المخصصة للعمل (الحواسيب)يمكن لأحد الموظفين تثبيت برنامج بدون ترخيص قد يكون يحتوي على برامج خبيثة ،وخطر تحميل البرامج المقرصنة تشكل خطر على المؤسسة.

المحور الخامس: مدى وعي الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة بالأمن المعلومات.

1_تختلف درجة وعي الموظفين بأهمية الأمن المعلوماتي يوجد موظفين لديهم درجة عالية من الوعي وهم المتمثلين في رؤساء الأقسام أو مسئولي الدوائر.

2_يوجد موظفين على درجة قليلة من الوعي تحرص المؤسسة في الأساس على أن لا تتوفر لديهم المعلومات الحساسة والسرية بل يمكن أن يحصلوا على معلومات سطحية لا تؤثر على الأمن المعلوماتي للمؤسسة.

3_هناك قانون داخلي للمؤسسة يحتوي على مجموعة من القوانين والعقوبات التي تضبط محاولة الاختراقات الأمنية وتسريب المعلومات.

4_تقوم المديرية العامة ببعث مراسلات للوكالات التابعة لها تحتوي على كل ماهو جديد ومتعلق بالأمن المعلوماتي ،وتقوم الوكالة بدورها بعمليات تحسيسية مباشرة وتضييق رقعة تداول المعلومة ،كل معلومة تعطى لصاحبها أو الدائرة التي تعنى بها ولا تتوفر لدى جميع دوائر الوكالة.

5_لا توفر المؤسسة تدريب للعاملين على الأنظمة المحوسبة لتطوير مهاراتهم المتعلقة بالمستجدات الأمنية.

6_يشمل عقد التوظيف للعاملين على مسئوليات ومهام الموظف تجاه الأمن المعلوماتي.

7_وجود قوانين تمنع الموظفين من تثبيت برامج غير مرخصة من طرف المؤسسة إذ اكتشف المهندس المسئول على الأمن اختراق لهذا القانون يعاقب الموظف .

8_يطلب من الموظف تبليغ دائرة الإحصاء والإعلام الآلي عند شكه بوجود ثغرة أمنية أو نقطة ضعف في احد الأنظمة وتقوم المديرية بعمل الإجراءات اللازمة لتصليحها.

9_لم تصادف المؤسسة خروقات أمنية وذلك بفضل تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمان المعلومات في المؤسسة وتختلف العقوبة المطبقة على حسب درجة خطأ العامل من(التحسيس،الردع،الخصم،الطرد).

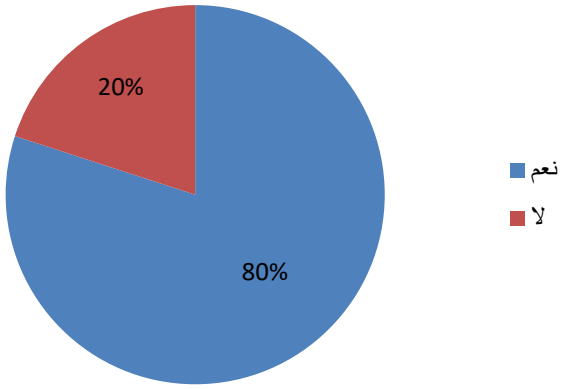
المبحث الثالث:عرض وتفسير البيانات الخاصة بالإستبيان.

المطلب الأول: محور البيانات الشخصية:

الجدول رقم 01: جدول يوضح توزيع مفردات عينة البحث حسب متغير الجنس.

الجنس	التكرار	النسبة المئوية
ذكر	12	٪80
أنثى	**3**	٪20
المجموع	15	**%100**

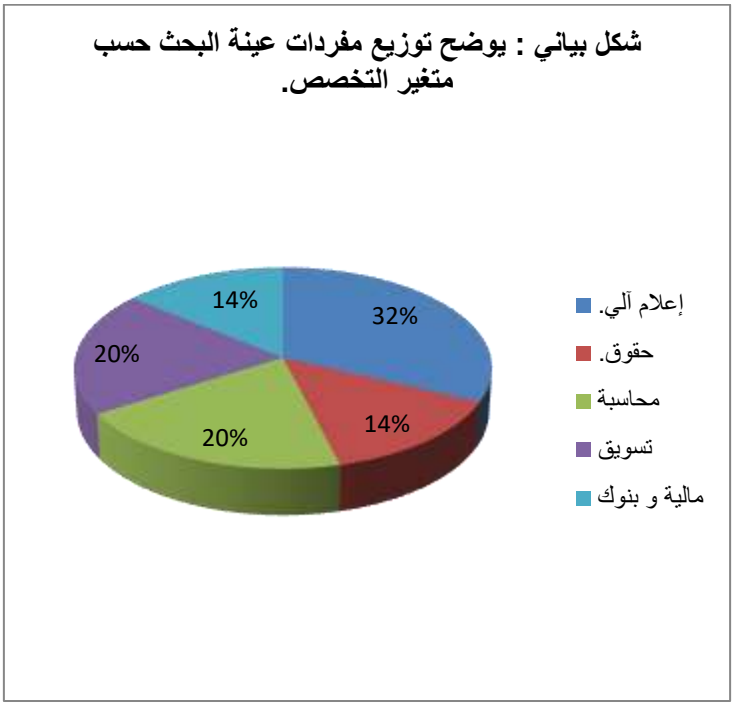
الشكل رقم1: توزيع مفردات البحث حسب متغير الجنس



يتبين من الجدول رقم 01 وشكله البياني المرافق أن أكبر نسبة من المبحوثين هي 80% ممثلة لـ 12 موظف من الذكور لتليها نسبة الإناث 20% الذين هم 3موظفات بالمؤسسة، ومنه نلاحظ أن عدد الذكور في مجتمع البحث أكبر من عدد الإناث،وهذا يبين أن المؤسسة تميل لتوظيف الذكور أكثر من الإناث وهذا ما توصلنا إليه من خلال المسح الشامل للموظفين الذي قمنا به عن طريق استمارة الاستبيان.

الجدول رقم 02: جدول يوضح توزيع مفردات عينة البحث حسب متغير التخصص.

التخصص	التكرار	النسبة المئوية
إعلام آلي	5	% 32
حقوق	2	14%
تسويق	3	20%
محاسبة	3	20%
مالية وبنوك	2	14%
المجموع	15	%100

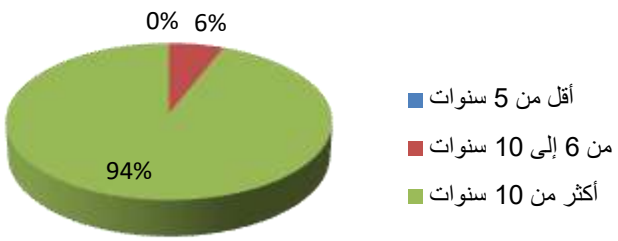


من خلال الجدول رقم 02 وشكله البياني نلاحظ أن أغلب المبحوثين الذين جاءت نسبتهم أكبر هم من تخصصي الإعلام الآلي والتسويق وجاءت نسبتهم متعادلة بـ26%، يليهم تخصص المحاسبة بنسبة 20% بينما تخصصي الحقوق والمالية والبنوك في الأخير بنسبة 14% ،ربما يرجع هذا لان تخصص الإعلام الآلي مهم بالنسبة لمختلف المؤسسات كون المتخصصين فيه هم القائمون على الحصول على المعلومات وتحليلها وتنظيمها واسترجاعها وحمايتها بمختلف أشكالها بالمؤسسة .

الجدول رقم 03: جدول يوضح توزيع مفردات عينة البحث حسب متغير الاقدمية.

المستوى الجامعي	التكرار	النسبة
أقل من5 سنوات	0	%0
من6الى10سنوات	1	%6
اكثرمن10سنوات	14	% 94
المجموع	15	%100

شكل بياني: يوضح توزيع مفردات عينة البحث حسب متغير الاقدمية.



يظهر من خلال قراءة الجدول رقم 03 و شكله البياني أن النسبة الأكبر جاءت للاقدمية أكثر من 10 سنوات بنسبة 94%، ونلاحظ أن تقريبا كل الموظفين باقدمية اكبر من 10سنوات ربما يرجع هذا أن المؤسسة انشئت قبل 12سنة ولم يتغير موظفيها منذ ذالك الوقت.

المطلب الثاني :المصادر التي تسهم في تكوين ثقافة الأمن المعلوماتي لدى الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

1/الأمن المعلوماتي حسب رأي المبحوثين يدور في النقاط التالية:

_تامين تداول المعلومات عبر شبكة الانترنت.

_هو الأساليب المتخذة من اجل حماية معلومات المؤسسة.

_هو مجموعة من الأدوات والإجراءات الأمنية التي تحمي معلومات المؤسسة من سوء الاستخدام أو التلف أو التعطيل.

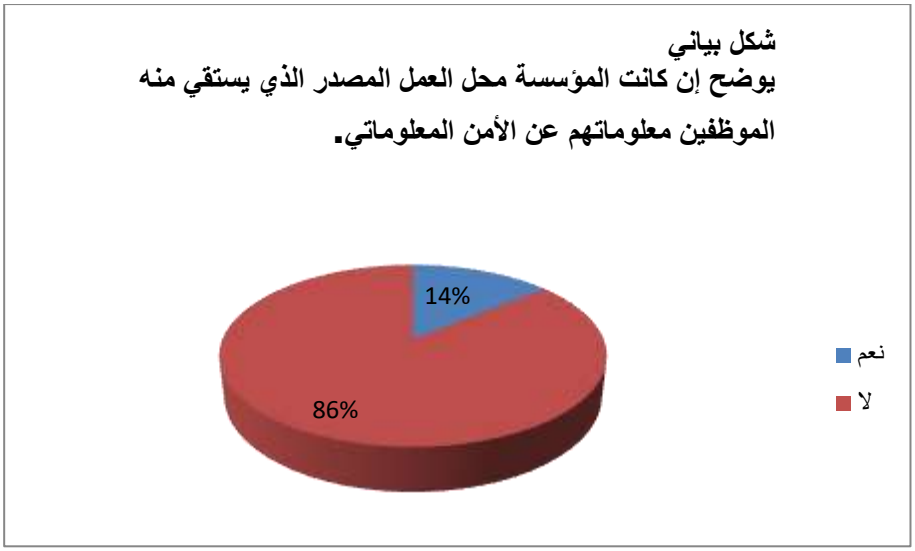
_العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها والحاجز الذي يمنع الاعتداء عليها.

_هي مجموعة الإجراءات الأمنية التي تحمي معلومات المؤسسة الحساسة.

* من خلال مجموعة التعريفات الموضحة أعلاه نلاحظ أن المبحوثين على درجة ثقافة واسعة حول ماهية الأمن المعلوماتي وضرورته بالمؤسسة ودرجة خطورته عليها.

الجدول رقم 04: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم02 ويوضح إن كان المؤسسة محل العمل المصدر الذي يستقي منه الموظفين معلوماتهم عن الأمن المعلوماتي.

هل تعد المؤسسة محل العمل المصدر الذي تستقون منه معلوماتكم حول الأمن المعلوماتي؟		
الإجابة	**التكرار**	**النسبة المئوية**
نعم	2	14%
لا	13	86%
المجموع	15	%100

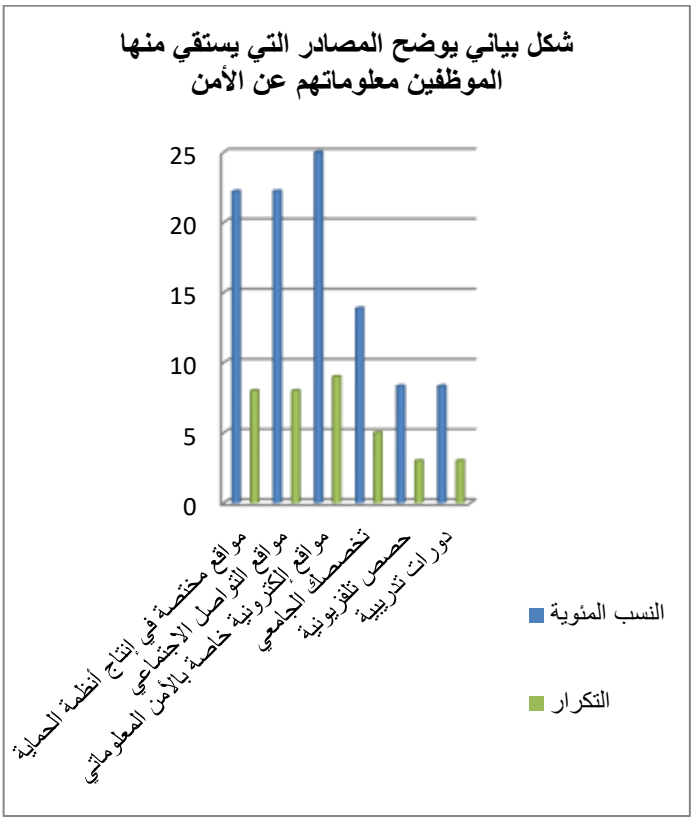


يتضح من خلال الجدول وتمثيله البياني أعلاه أن اغلب المبحوثين أجابوا ب"**لا**" بنسبة 86% وهذا يعني أن المؤسسة محل العمل ليست المصدر الذي يستقي منه الموظفين معلوماتهم عن الأمن المعلوماتي وهذا يتنافى مع نتائج المقابلة والتي اكدت على حرص المؤسسة على توعية الموظفين وامدادهم بالمعلومات عن الامن المعلوماتي، بينما الذين أجابوا ب"نعم" كانوا بنسبة14% ربما هذا يعود لمناصبهم الحساسة في المؤسسة ويجب عليها أن تزود الموظف بمعلومات عن الأمن المعلوماتي وكل المستجدات فيه.

الجدول رقم 05: جدول يوضح خيارات مفردات عينة البحث على السؤال التابع للسؤال رقم02 إذا كانت إجابتهم "لا"

ويوضح المصادر الأخرى التي يستقي منها الموظفين معلوماتهم عن الأمن المعلوماتي

إذا كانت إجابتك "نعم " ففيم تتمثل هذه المصادر ؟		
البدائل	**التكرار**	**النسبة المئوية**
مواقع مختصة في إنتاج أنظمة الحماية	08	22.22%
مواقع التواصل الاجتماعي	08	22.22%
مواقع إلكترونية خاصة بالأمن المعلوماتي	09	25%
تخصصك الجامعي	05	13.88%
حصص تلفزيونية	03	8.33%
دورات تدريبية	03	8.33%
مصادر أخرى	00	00%
المجموع	36	99.98%



بعد قراءة الجدول رقم 05 وتمثيله البياني أعلاه نلاحظ أن النسبة الأكبر تخص الخيارين التاليين مواقع إلكترونية خاصة بالأمن المعلوماتي بنسبة25% تليها مواقع التواصل الاجتماعي بنسبة08% ويرجع مجيء خيار مواقع الكترونية خاصة بالأمن كأكبر نسبة بسبب التغيرات والتحديثات المستمرة في هذه المجالات، إضافة إلى أنه أصبحت هناك مخاطر وتهديدات تواجه المستخدمين يمكن التعرف عليها والتعامل معها من خلال استقاء المعلومات عنها من هذه المواقع،أما مواقع التواصل الاجتماعي بعدها لأن هذه المواقع هي أكثر الأنشطة شعبية على الانترنت التي

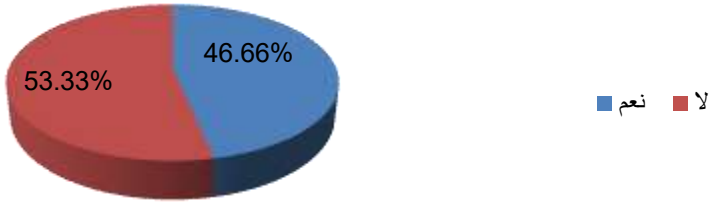
ينخرط فيها المستخدمون حيث تظهر إحصائيات وسائل التواصل الاجتماعي لعام 2019 أن هناك 3.5 مليار مستخدم لهذه الوسائل في جميع أنحاء العالم، وهذا العدد في تزايد حيث يعادل هذا العدد نسبة 45% من سكان العالم الحاليين.[1]

أما بالنسبة لخيار "مواقع مختصة في إنتاج أنظمة الحماية" والذي جاءت نسبته بـ 22.22% كون هاته المواقع أصبحت ذات أهمية كبيرة في إنتاج برمجيات مضادة للفيروسات وتكشف المتطفلين على الأجهزة، أما مجيء خيار " التكوين في إطار تخصصك الجامعي" بنسبة تقدر بـ 13.88% تظهر هذه النتيجة بأن الموظفين لا يعتمدون على مايتلقونه من معلومات في إطار تخصصهم الجامعي فقط حيث أصبحت الانترنت بكل ما تحتويه من مواقع الكترونية تعدد وتنوع المصادر التي تشرح المعلومات والمواضيع بأشكال مختلفة.

الجدول رقم 06: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم03 ويوضح إن كانت المؤسسة محل العمل تقوم بتجديد معلومات الموظفين عن الأمن المعلوماتي.

هل تقوم المؤسسة بتجديد معلوماتكم حول الأمن المعلوماتي؟		
الإجابة	**التكرار**	**النسبة المئوية**
نعم	7	46.66%
لا	8	53.33%
المجموع	15	%100

شكل يوضح إن كانت المؤسسة محل العمل تقوم بتجديد معلومات الموظفين عن الأمن المعلوماتي



[1] Maryam Mohsin, 10 Social Media Statistics You Need to Know in 2020, https://www.oberlo.com/blog/social-media-marketing-statistics , 11-08-2020, 09:45h

بعد قراءة الجدول رقم06 وتمثيله البياني، نلاحظ أن الإجابة "لا"كانت إجابة اكثر من نصف اموظفين بنسبة 53.33%الامن المعلوماتي ومختلف التطورات الحاصلة فيه بل يكفيهم أن يكونوا على دراية بماهيته فقط يمكن أن يعود هذا لطبيعة عملهم والمهام المكلفين بها والتي يمكن أن لا تحتاج لتجديد معلوماتهم حول تليها "نعم" بنسبة46.66% ويمكن أن يعود هذا لطبيعة عمل هؤلاء الموظفين الحساسة والتي يجب أن يكونوا فيها على دراية بمختلف التطورات في أنظمة الحماية ومجال الاختراق.

الجدول رقم 07: جدول يوضح خيارات مفردات عينة البحث على السؤال التابع للسؤال03

ويوضح إذا كانت المؤسسة محل العمل تقوم بتجديد معلومات الموظفين عن الأمن المعلوماتي بصورة ما.

إذا كانت الإجابة "نعم" فكيف يكون ذلك :		
البدائل	**التكرار**	**النسبة**
بصورة دورية منتظمة	0	00%
عند الضرورة	7	100%
أخرى	0	00%
المجموع	7	100%

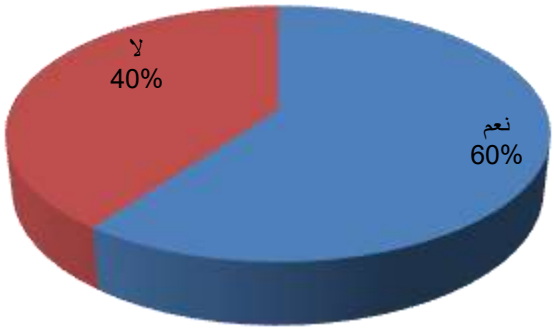
بعد قراءة الجدول رقم 07 وتمثيله البياني، توصلنا إلى انه إذا كانت الإجابة "نعم" فانه بنسبة100% للخيار بصورة دورية منتظمة أي أن كل المبحوثين الذين أجابوا ب"نعم" تقوم المؤسسة بتجديد معلوماتهم عن الأمن المعلوماتي فذالك يكون عند الضرورة يمكن أن يرجع ذالك لطبيعة عملهم التي تحتاج لتجديد معلوماتهم عند حدوث مشاكل في الأمن المعلوماتي أو عند وجود أنظمة حماية جديدة أو غير ذالك

المطلب الثالث: امتلاك الموظف لمعلومات حول أساليب وطرق الاختراق

الجدول رقم 08: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم 01

هل تمتلك معلومات حول طرق وأساليب الاختراق ؟		
الإجابة	**التكرار**	**النسبة المئوية**
نعم	09	60%
لا	06	40%
المجموع	15	%100

شكل يوضح امتلاك الموظف لمعلومات حول أساليب وطرق الاختراق



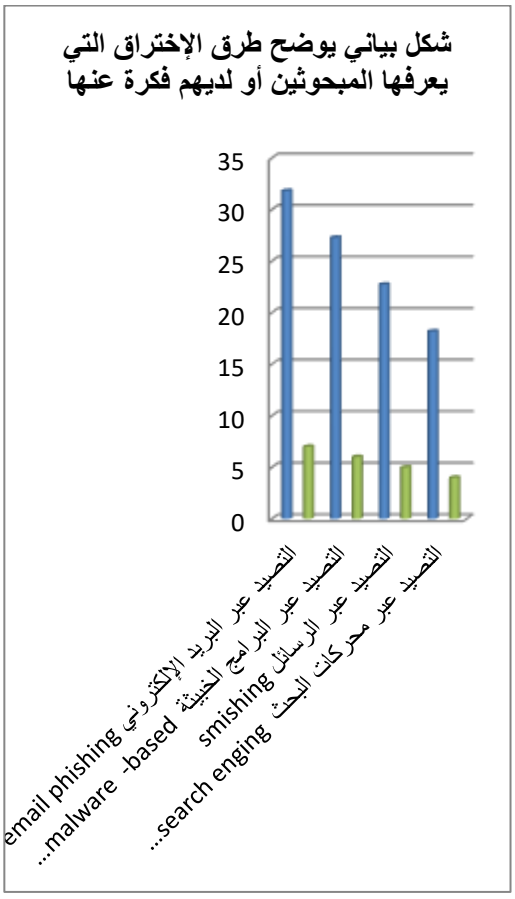
بعد قراءة الجدول رقم 08 يتضح أن أكبر نسبة 60% كانت للإجابة "نعم" في حين "لا" فجاءت بأقل نسبة 40 %، وهذا يعني أن اغلب الموظفين على دراية بأساليب وطرق الاختراق وهذا ربما قد يعود إلى أن العصر الذي نعيش فيه يتغير باستمرار خاصة على مستوى التكنولوجيا التي أصبحت تحتم على جميع من يتعامل وسائل التكنولوجيا الحديثة أن يمتلك معلومات حول الأمن المعلوماتي، الذي تظهر فيه كل يوم أساليب جديدة للاختراق والتجسس والتعدي على الخصوصية الفردية والابتزاز..الخ، مما يحتم على من يستخدم التكنولوجيات الحديثة للإعلام والاتصال

أن يبقى على اطلاع بكل ما يستجد في هذا المجال من المخاطر ومن الآليات للتصدي لها ومواجهتها أو الاحتياط والوقاية منها.

الجدول رقم 09: جدول يوضح خيارات مفردات عينة البحث على السؤال التابع للسؤال01.

ويوضح طرق الاختراق التي يعرفها المبحوثين أو لديهم فكرة عنها.

من بين طرق الاختراق التالية، أيها لديك فكرة عنها؟		
البدائل	التكرار	النسبة المئوية
التصيد عبر البريد الالكتروني Email phishing	7	% 31.81
التصيد عبر البرامج الخبيثة Malware-Based phishing	6	% 27.27
التصيد عبر الرسائل النصية SMishing	5	% 22.72
التصيد عبر محركات البحث Searh Enging phishing	4	% 18.18
المجموع	22	% 99.98



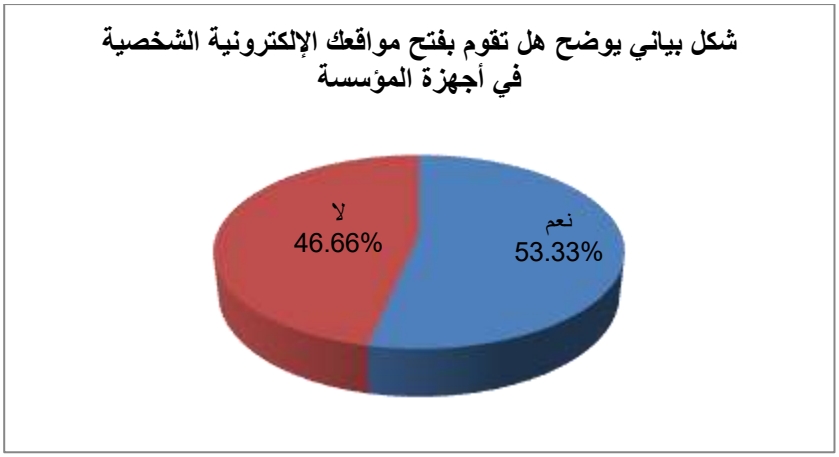
من خلال قراءة الجدول رقم 09 وتمثيله البياني،يتضح أن أعلى نسبة 31.81 % جاءت لخيار "التصيد عبر البريد الالكتروني" ويعود سبب ذلك أن البريد الالكتروني من بين أبرز خدمات الانترنت شهرة واستخداما، إضافة إلى أن أغلب الأجهزة الإلكترونية مثل الهواتف الذكية ومواقع الانترنت مثل مواقع التواصل الاجتماعي تعمل به أو تطلبه في عملية التسجيل في خدماتها، مما يجعل الأشخاص عرضه لمثل هذه الهجمات، كما أن مواقع الانترنت بصفة عامة

ومواقع الأمن المعلوماتي وبرامج الحماية تحذر منها باستمرار، ثم تليها نسبة 27.27% لخيار التصيد عبر البرامج الخبيثة، هذا يرجع إلى أن المبحوثين أكثر عرضه لمثل هذه المخاطر لأنه في أغلب الأحيان عند تثبيت أحد البرامج أو التطبيقات عبر موقع من المواقع الالكترونية، قد يكون ذلك المواقع يحمل أحد الفيروسات الخبيثة التي تدخل عن طريق تحميل تطبيق أو برنامج معين،[2] أما خيار "التصيد عبر الرسائل النصية" جاءت نسبته بـ 22.72% قد يعود ذالك لان هاته الخاصية تعمل على جمع معلومات شخصية عن ضحايا مستهدفين وذلك بإرسال روابط ضارة أو إرسال مكالمة هاتفية بأرقام مزيفة أو مكالمة آلية وتطلب من المستخدمين بعض المعلومات مستغلين افتقارهم للوعي الكافي لخداعهم، أما خيار "التصيد عبر محركات البحث" جاءت نسبته بـ 18.18% في الأخير وقد يعود ذلك أن هذا النوع لم يصادفهم وحتى وإن كان شائع جدا حيث يقوم فيه المحتالين بنقل مستخدمي هذه المحركات من الموقع الرئيسي إلى موقع ويب مفخخ لتصيد معلوماته.

الجدول رقم 10: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم 03

هل تقوم بفتح مواقعك الالكترونية الشخصية في أجهزة المؤسسة ؟		
الإجابة	**التكرار**	**النسبة المئوية**
نعم	08	53.33%
لا	07	46.66%
المجموع	15	%100

[2] 100مليون رسالة بريد إلكتروني احتيالية تستهدف المستخدمين يوميا، متاح على الرابط: https://www.aleqt.com/2020/04/21/article_1809911.html، تاريخ الزيارة: 08-08-2020، على الساعة: 17:30

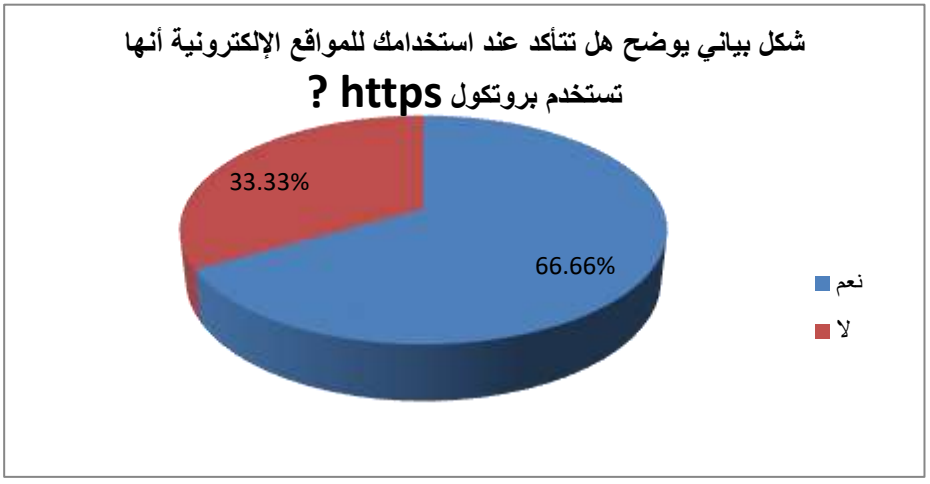


يوضح الجدول رقم 10 وتمثيله البياني، الخاص بقيام الموظفين بفتح مواقعهم الالكترونية الشخصية في أجهزة المؤسسة تتم عادة لدى 53.33% من مفردات عينة الدراسة ربما هذا يرجع لتوفر شبكة ويفي(wifi) مجانية بالمؤسسة وهذا قد يعرض المؤسسة لخطر كبير إن كان الجهاز الذي يفتحون عليه مواقعهم يحمل معلومات هامة فقد يتم اختراق مواقعهم بالتالي اختراق امن المؤسسة ، أما 46.66% فلا يقومون بهذا الفعل عادة،ربما يعود هذا لامتلاكهم لهواتف محمولة خاصة أو أجهزة حواسيب شخصية ولا يقومون بفتح مواقعهم الشخصية في المؤسسة ربما لامتلاكهم انترنت على أجهزتهم الشخصية أو للحفاظ على خصوصيتهم.

الجدول رقم 11: جدول يوضح خيارات مفردات عينة البحث على السؤال التابع للسؤال03

ويوضح تأكد المبحوثين من استخدام المواقع الإلكترونية لبروتوكول HTTPS عند قيامهم بفتح مواقعهم الشخصية في أجهزة المؤسسة.

هل تتأكد عند استخدامك للمواقع الالكترونية أنها تستخدم بروتكول"Https"؟		
البدائل	**التكرار**	**النسبة المئوية**
نعم	10	66.66%
لا	05	33.33%
المجموع	15	%100



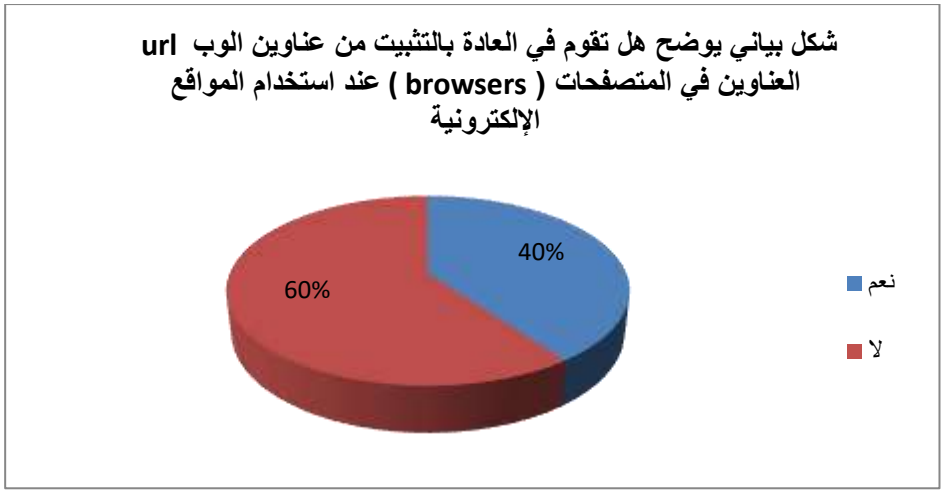
يوضح الجدول رقم 11وتمثيله البياني أن المتعلق بتأكد الموظفين عينة الدراسة عند استخدامهم المواقع الالكترونية أنها تستخدم بروتوكول HTTPS، أن 66.66% من المبحوثين يتأكدون من هذا الأمر بينما 33.33% لا يقومون بهذا الفعل، واستخدام الموظفين لمواقع تحتوي بروتوكول HTTPS يدل على أنهم يحاولون الحافظ على معلوماتهم الخاصة ومعلومات المؤسسة بمنع أي جهة مجهولة الوصول لها وبهذا يستخدمونها بأمن وبدون إزعاج من طرف المتطفلين، ويعتبر بروتوكول HTTPS بروتوكول نقل النص التشعبي الآمن، بحيث يسمح

بتصفح المواقع بدرجة أعلى من الأمان، وانتباه أغلب الموظفين لهذا الأمر يدل على درجة مقبولة من ثقافة الأمن المعلوماتي لديهم .

الجدول رقم 12: جدول يوضح إجابة مفردات عينة البحث على السؤال التابع للسؤال رقم 3

ويوضح إن كان المبحوثين يتثبتون من عناوين الوبURL في شريط عناوين المتصفحات**(Browsers)**.عند قيامهم بفتح مواقعهم الشخصية في أجهزة المؤسسة

هل تقوم في العادة بالتثبيت من عناوين الوب URL في شريط العناوين في المتصفحات (Browsers) عند استخدام المواقع الإلكترونية؟		
البدائل	**التكرار**	**النسبة المئوية**
نعم	06	40%
لا	09	60%
المجموع	15	%100

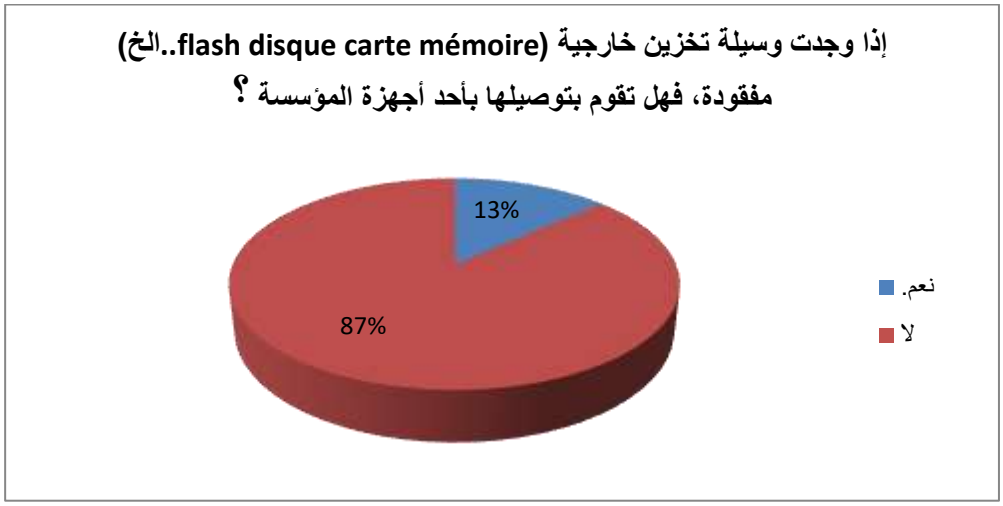


يوضح الجدول رقم12 وشكله البياني أن أغلب الإجابات جاءت بـ "لا"بنسبة 60% أما "لا" بنسبة 45.26 % وهذا يبين أن الموظفين لا يتثبتون من عناوين الوب، وهذا قد يشكل خطر عليهم وخطر اكبر على معلومات المؤسسة، لأن عملية التصيد تتم أحيانا من خلال صفحات مزورة لبعض المواقع ، مثل بعض الصفحات التي يعتقد مستخدمها أنها صفحة واجهة الفايسبوك، فيدخل فيها اسم المستخدم و كلمة المرور، مما يعرضه للاختراق لاحقا. ويمكن اكتشاف أن الصفحة مزورة من خلال عنوان URL الخاص بها، وبالتالي عدم تثبت أغلبية الموظفين من هذا العنوان، ومعرفة إن كان يطابق العنوان الرسمي للصفحة أو الموقع، يسهل تعرضهم للاختراق.

الجدول رقم 13: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم 04

ويوضح إن كان المبحوثين يقومون بتوصيل وسائل التخزين الخارجة، التي يجدونها مفقودة، بأحد أجهزة المؤسسة.

إذا وجدت وسيلة تخزين خارجية (flash disque carte mémoire..الخ) مفقودة، فهل تقوم بتوصيلها بأحد أجهزة المؤسسة ؟		
البدائل	**التكرار**	**النسبة**
نعم	02	13.33%
لا	13	86.66%
المجموع	15	%100

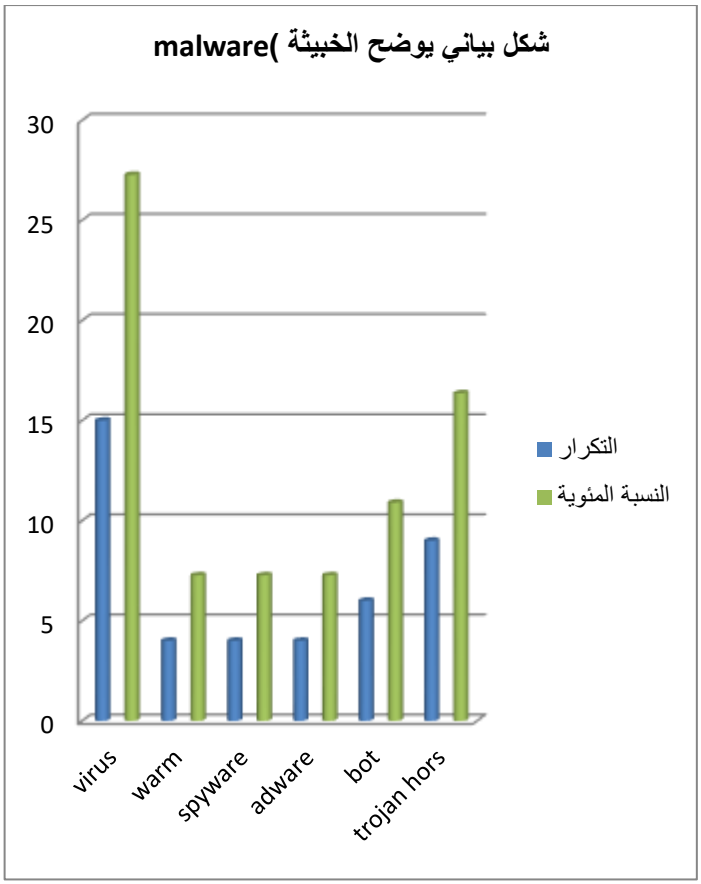


يوضح الجدول رقم13 وتمثيله البياني إجابة أغلب المبحوثين بـ "لا" وبنسبة 86.66 %على السؤال "إذا وجدت وسيلة تخزين خارجية مفقودة هل تقوم بتوصيلها بأحد أجهزة المؤسسة "، أما الإجابة بـ "نعم" فكانت بنسبة 13.33%، وتعود إجابة اغلب المبحوثين بنعم فيرجع السبب إلى أن أغلبهم يريد حماية المؤسسة من

المخاطر المختلفة، لأنها تشكل خطرا على أجهزتها فقد تحتوى فيروسات أو برامج خبيثة، وكذلك لأنهم يعتقدون أنه من باب الخصوصية والأخلاق عدم استخدام الشخص الشيء الذي ليس ملكا لهم. ،أما الذين أجابوا"نعم" فقد يعود إلى فضولهم الكبير ومحاولة التعرف على المحتوى الموجود في وسيلة التخزين أو لمعرفة هوية صاحب الوسيلة المفقودة وإرجاعها له.

الجدول رقم14: جدول يوضح إجابة مفردات عينة البحث على السؤال رقم 04 ويوضح البرامج الخبيثة (MALWARE) التي يعرف الموظفين معناها.

من بين البرامج الخبيثة (MALWARE) التالية أيها أنت على دراية بمعناها ؟		
البدائل	التكرار	النسبة المئوية
VIRUS	15	%27.27
Warm	4	7.27%
Spyware	4	7.27%
Adware	4	7.27%
Bot	6	10.90%
Trojan horse	9	16.36%
Fake antivirus	4	7.27%
Backdoor	3	5.45%
Rootkit	2	3.63%
Ransomware	4	7.27%
المجموع	55	99.96%



يوضح الجدول رقم 22 وتمثيله البياني أن أعلى نسبة من إجابات المبحوثين جاءت لخيار virus بنسبة 27.27%، وهذه النتيجة قد تعود لكون أن هذا البرنامج من أكثر البرامج شيوعا وغالبا يكون السبب وراء اختراق وإتلاف العديد من المواقع الالكترونية واختراق الأجهزة، ولكن يلاحظ بالمقابل أن واحدا من البرامج الخبيثة الذي يتم الحديث عنه بكثرة في السنوات الأخيرة، نظرا للخسائر المالية التي يسببها للأفراد والشركات، وهو فيروس الفدية Ransomware يبقى معروفا لدى 7.27% فقط من المبحوثين، أي في آخر ترتيب البرامج الخبيثة التي يعرفها الموظفين، وهو ما يجعلهم عرضة لأن يقعوا ضحايا لهذا النوع من البرامج الخبيثة التي تشهد انتشارا واسعا، ليس لهدف تخريبي محض وإنما بهدف جمع المال من الضحايا مهما كانت طبيعتهم وهذا قد يشكل خطر على المؤسسة والتي تعتبر اقتصادية بالدرجة الأولى، ويلاحظ عموما من نتائج الجدول أنه فيما عدا الفيروسات فإن معرفة أغلب الموظفين ضعيفة ببقية البرامج الخبيثة الأخرى.

المبحث الرابع:الاستنتاجات العامة للدراسة.

المطلب الأول :النتائج الخاصة بالمقابلة.

تعبر الوكالة الوطنية لتسيير القرض المصغر من أهم هياكل دعم وتعزيز المؤسسات الصغيرة والمتوسطة في الجزائر حيث تهدف إلى منح قروض مصغرة إلى الشباب الراغب في إنشاء مشاريع مصغرة.

تعتمد المؤسسة على مجموعة من الإجراءات والوسائل لحماية معلوماتها من خلال:

_جملة من أساليب الحماية المادية: المتمثلة في تسخير العنصر البشري داخل المؤسسة المتمثل في أعوان الأمن الذين يعملون بالتناوب ودون توقف ليلا ونهارا، للمحافظة على الأمن المادي للمؤسسة ككل المتمثل في (مقر المؤسسة،التجهيزات ،العتاد،الأفراد)، تخصيص أماكن لحماية وحفظ المعلومات والبيانات التي تتوفر عليها المؤسسة(السجلات،العتاد،أجهزة الإعلام الآلي،آلات النسخ،الخواتيم)وحمايتها من المخاطر الطبيعية عن طريق عمل نسخ احتياطية.

_وأخرى تقنية:بوضع جملة من أساليب الحماية البرمجية والمتمثلة في:

برامج مكافحة الفيروسات، تشفير البيانات :،المحافظة على امن الشبكة،4)التوثيق متعدد البرامج ،عمل لنسخ احتياطية،تصحيح البرامج،توفير مصدر احتياطي للطاقة الكهربائية.

_و أساليب أخرى للحماية التنظيمية والإدارية:عن طريق

1_تصنيف المعلومات حسب درجة سريتها وأهميتها.

2_التوعية داخل المؤسسة:من خلال القيام بعمليات تحسيسية مباشرة وتضييق رقعة تداول المعلومة.

3_وضع سياسة أمنية للمؤسسة تنص على:

_ ضرورة أمن المعلومات المهنية و الشخصية.

_وضع مجموعة من_التدابير التي يجب اتخاذها عند أداء مهمة إلى الخارج.

_ قوانين تسير نقل البيانات:بهدف حماية البيانات و المعلومات المنقولة في الشبكة المعلوماتية.

_التحكم في استعمال الانترنت على مستوى الإدارة أو المؤسسة و ضمان حماية أنظمة الإعلام من الهجمات الالكترونية.

_استخدام الانترنت لأغراض مهنية فقط.

_وضع مجموعة من القواعد لاستخدام وسائل التواصل الاجتماعي بالمؤسسة.

_ تامين الاتصال: لحماية و تامين المعلومات و البيانات السرية

_ اقتناء ووضع البرمجيات:للحد من الخطر المتعلق بأمن أنظمة الإعلام عند اقتناء و وضع برمجيات.

_ إدارة البيانات وحفظها.

تسند مهمة حماية المعلومات بالمؤسسة إلى الدائرة المكلفة بالإحصاء والإعلام الآلي يشرف على هذه الدائرة مهندس إحصاء، ومهندس إعلام ألي مهمته المحافظة على الأمن المعلوماتي للمؤسسة من خلال: المحافظة على سرية البيانات والمعلومات وسلامتها من التغيير أو التعديل فيها واستمرارية توفرها في حال ما احتاجت المؤسسة الوصول إليها من خلال توفير برامج الأمن وأساليب الحماية وكذالك مراقبة قاعدة المعطيات، لكل دائرة في المؤسسة معلومات وبيانات خاصة بها لا يمكن لأي دائرة التصريح ببياناتها لدائرة أخرى، تختلف أشكال المعلومات و سريتها حسب الجهات الموجودة بالمؤسسة

تختلف درجة حماية المعلومات بالمؤسسة حسب سريتها وأهميتها فهناك معلومات لا تحتاج إلى حماية مطلقا،ومعلومات تحتاج إلى درجة معينة من الحماية ،وهناك معلومات تتطلب حماية قصوى.

تهدد الأمن المعلوماتي للمؤسسة مجموعة من المخاطر الطبيعية وأخرى معلوماتية وتقنية،وأخرى بشرية متمثلة في قلة وعي الموظفين.

تختلف درجة وعي الموظفين بأهمية الأمن المعلوماتي يوجد موظفين لديهم درجة عالية من الوعي، ويوجد موظفين على درجة قليلة من الوعي، هناك قانون داخلي للمؤسسة يحتوي على مجموعة من القوانين والعقوبات التي تضبط محاولة الاختراقات الأمنية وتسريب المعلومات، لم تصادف المؤسسة خروقات أمنية.

المطلب الثاني:النتائج الخاصة بالاستبيان.

بعد تحليل البيانات المتحصل عليها ،تمكننا من استنتاج عدة نقاط هامة حول ثقافة الأمن المعلوماتي لدى الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة وتوصلنا إلى أن:

_عدد الذكور في مجتمع البحث أكبر من عدد الإناث،وهذا يبين أن المؤسسة ربما تميل لتوظيف الذكور أكثر من الإناث.

_أغلب الموظفين هم من تخصصي الإعلام الآلي والتسويق ،يليهم تخصص المحاسبة، بعده تخصصي الحقوق والمالية والبنوك في الأخير.

_كل الموظفين تقريبا باقدمية اكبر من 10سنوات.

_توصلنا إلى أن المبحوثين على درجة ثقافة واسعة حول ماهية الأمن المعلوماتي وضرورته بالمؤسسة ودرجة خطورته عليها.

_وجدنا أن المؤسسة محل العمل ليست المصدر الذي يستقي منه اغلب الموظفين معلوماتهم عن الأمن المعلوماتي،بل يلجئون إلى بدائل أخرى تخص الخيارين التاليين: مواقع إلكترونية خاصة بالأمن المعلوماتي ،تليها مواقع التواصل الاجتماعي ،و خيار "مواقع مختصة في إنتاج أنظمة الحماية" والذي جاء بعده ،يليه خيار " التكوين في إطار تخصصك الجامعي" .

_كانت إجابة النصف من الموظفين بان المؤسسة لا تقوم بتجديد معلوماتهم حول الأمن المعلوماتي ومختلف التطورات الحاصلة فيه، بينما الموظفين المتبقين اجابو بأنها تقوم بتجديد معلوماتهم فيه عند الضرورة،ويمكن أن يعود هذا لطبيعة عمل هؤلاء الموظفين الحساسة .

_اغلب الموظفين بالمؤسسة على دراية بأساليب وطرق الاختراق الالكترونية، يتضح أن أعلى نسبة جاءت لخيار "التصيد عبر البريد الالكتروني" ويعود سبب ذلك أن البريد الالكتروني من بين أبرز خدمات الانترنت شهرة واستخداما، ثم يليه خيار التصيد عبر البرامج الخبيثة، هذا يرجع إلى أن المبحوثين أكثر عرضه لمثل هذه

المخاطر لأنه في أغلب الأحيان عند تثبيت أحد البرامج أو التطبيقات عبر موقع من المواقع الالكترونية، أما خيار "التصيد عبر الرسائل النصية" جاءت نسبته بعده ،أما خيار "التصيد عبر محركات البحث" جاء في الأخير وقد يعود ذلك أن هذا النوع لم يصادفهم وحتى وإن كان شائع جدا.

_يقوم اغلب الموظفين بفتح مواقعهم الالكترونية الشخصية في أجهزة المؤسسة ربما هذا يرجع لتوفر شبكة ويفي(wifi) مجانية بالمؤسسة أما الأقل فلا يقومون بهذا الفعل عادة،ربما يعود هذا لامتلاكهم لهواتف محمولة خاصة أو أجهزة حواسيب شخصية،ويتأكد اغلب الموظفين الذين يقومون بفتح حساباتهم الشخصية في المؤسسة من استخدام هاته المواقع لبروتوكول HTTPS وهذا يدل على وجود حس امني لديهم،لكنهم بالمقابل لا يتثبتون من عناوين الوب URL في شريط العناوين في المتصفحات (Browsers) عند استخدام هاته المواقع الإلكترونية وهذا قد يشكل خطر عليهم وخطر اكبر على معلومات المؤسسة.

_توصلنا إلى أن اغلب المبحوثين لا يقومون بتوصيل وسيلة تخزين خارجية (flash disque carte mémoire..الخ)إذا وجدوها مفقودة كونها تشكل خطرا على أجهزة المؤسسة فقد تحتوى فيروسات أو برامج خبيثة.

_اغلب المبحوثين على دراية بالبرامج الخبيثة malware وعلى رأسها الفيروسvirus وهذه النتيجة قد تعود لكون أن هذا البرنامج من أكثر البرامج شيوعا وغالبا يكون السبب وراء إتلاف واختراق الأجهزة.

خاتمة

خاتمة:

تمثل تكنولوجيا المعلومات المرتكز الاستراتيجي الأساسي في خطط البناء والتنمية ،وهي مخازن لمليارات الصفحات من المعلومات السياسية ،التاريخية،التجارية إلى غير ذالك ،ولا عجب أن تتسابق أعظم المؤسسات والهيئات لتضمن موقع ضمن هذه الشبكة ،حيث تعتبر المعلومات من أهم أساسيات المؤسسة التي يجب حمايتها عن طريق وضع سياسة أمنية وإستراتيجية لحمايتها من مختلف المخاطر التي قد تهدد الأمن المعلوماتي لها والذي يعتبر من بين أهم المواضيع في وقتنا الحالي لأنه يمس بشكل مباشر حياة كل المتعاملين مع التكنولوجيات الحديثة سواء كانوا أشخاص أو مؤسسات،و التي تقوم بوضع مجموعة من الإجراءات والأدوات التي تسمح بحماية موارد النظام وقواعد البيانات والأجهزة والخوادم وغيرها من كل أشكال الاستخدام الغير الشرعي للمعلومات ،وضمان توافرها وسريتها وسلامتها .وتعتبر الوكالة الوطنية لتسيير القرض المصغر من بين المؤسسات التي تعتمد على تكنولوجيا المعلومات وقامت بدورها بوضع إستراتيجية أمنية،تمثلت في مجموعة من الأساليب والوسائل لحماية معلوماتها تمثلت في مجموعة من وسائل الحماية المادية والبرمجية والتنظيمية والإدارية،وكذا تتبع سياسة أمنية خاصة تفرض على الموظفين والمتعاملين تطبيقها،بالإضافة إلى توعيتهم بضرورة تطبيقها لتجنب مختلف الخروقات والأخطار الأمنية بمختلف أنواعها.

قائمة المصادر والمراجع

القواميس والمعاجم:

1_المنجد في اللغة العربية، الطبعة 31، بيروت دار المشرق، 1991 .

2_ابن منظور،لسان العرب:المجلد الأول،دار الحديث ،القاهرة،2003.

الكتب بالغة العربية:

3_أحمد أبو اسعد،د.سلطان النوري،دراسة الحالة في إطار جديد،مركز ديبونو لتعليم التفكير عضو اتحاد الناشرين العرب،عمان/دبي،2016.

4_حكمت رشيد سلطان،محمود محمد أمين عثمان :الإدارة الإستراتيجية، شركة دار الأكاديميون للنشر والتوزيع،2019.

5_سعد سلمان المشهداني،منهجية البحث العلمي،ط1،الأردن ،دار أسامة للنشر والتوزيع ،2019.

6_صلاح عبد القادر النعيمي،الإستراتيجية والإدارة الإستراتيجية نظرة تحليلية وعلاقات تكاملية للمفاهيم والمصطلحات،دار اليازوري للنشر والتوزيع 2021.

7_عدنان مصطفى البار،خالد علي المرحبي:أمن المعلومات والأمن السيبراني، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز.

8_محمد عبد السلام،مناهج البحث في العلوم الاجتماعية والانسانية،مكتبة نور،2020.

9_محمود احمد درويش،مناهج البحث في العلوم الإنسانية،مؤسسة الأمة العربية للنشر والتوزيع ،مصر،2018.

10_مروان عبد المجيد إبراهيم،أسس البحث العلمي لإعداد الرسائل الجامعية ،مؤسسة الوراق ،عمان ، 2000.

الأطروحات والرسائل والمذكرات:

12_أيمن محمد فارس الدنف: واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، الجامعة الإسلامية– غزة عمادة الدراسات العليا كلية التجارة قســم إدارة الأعمال، قدمت هذه الدراسة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية بغزة – كلية التجارة،2013.

13_د.جمال بوازدية ،الأمن السيبراني،محاضرات مقدمة لطلبة السنة الثانية ماستر تخصص دراسات إستراتيجية وأمنية،جامعة الجزائر–3–كلية العلوم السياسية والعلاقات الدولية،2020–2021.

14_د.مرمي مراد، محاضرات في مقياس :نظم المعلومات، جامعة فرحات عباس سطيف–1 كلية العلوم الاقتصادية والتجارية وعلوم التسيير قسم العلوم الاقتصادية السنة الأولى ماستر تخصص: اقتصاد وتسيير المؤسسات، 2023/2022.

15_وراد زواوي،منهجية إعداد مذكرة تخرج موجهة لطلبة السنة الثانية ماستر،جامعة الجيلالي اليابس سيدي بلعباس ،كلية العلوم الاقتصادية والتجارية وعلوم التسيير،تخصص مالية وتجارة دولية تسويق مصرفي،قسم العلوم التجارية،2021/2020.

الكتب بالغة الأجنبية:

16_Martin C.Libicki,Conquest in Cyberspace:National Security and Information Warfare.(New York:Cambridge University Press,2007)

ftp://gftp.ga/the%20allEmbaracing%20library/establishment/pdf

.

المجلات والدوريات:

17_آمال بن اعراب،الخطر المعلوماتي ومسؤولية حماية المعلومة في المؤسسة الاقتصادية،جامعة الجزائر 3،مجلة المعيار،المجلد:25،العدد:55،2021

41 الوصول تاريخ /07/ 97 القبول 9042 /07/ 41 الخط علي النشر 9090 /00/ 9094

Received 41/07/9042 Accepted 97/07/9090 Published online 15/03/2021

18_إيمان بغدادي تطبيق قانون المنافسة على المؤسسة العمومية الاقتصادية ، مجلة التحولات الاقتصادية العدد: 02،المجلد:01،جامعة قسنطينة، ، 39 معهد العلوم الاقتصادية والتجارية وعلوم التسيير – المركز الجامعي مرسلي عبد الله . تيبازة,

dz edu .umc@baghdadi.imene.

19_سعد علي الحاج علي بكري،» الأمن السيبراني ومعضلة حمايته ..عولمة التعليم العالي ..الرقمي« ، جريدة العرب الاقتصادية الدولية،العدد 25 ، 24 (أوت 2017)..

20_عتيقة بن طاطة،مساهمة نظم المعلومات في عمليات إدارة المعرفة:مقاربة نظرية،كلية العلوم الاقتصادية وعلوم التسيير ،جامعة معسكر،مجلة التنويع

الاقتصادية،المجلد04،العدد01،جامعة عين تموشنت_بلحاج بوشعيب، الجزائر ،2023.

21_عوابدي عمار،القانون الإداري ،الجزء الأول،ط5،ديوان المطبوعات الجامعية،2008 .

22_عيسى يونسي،سامية شينار عائشة عماري،العينة وأسس المعاينة في البحوث الاجتماعية،مجلة الرواق للدراسات الاجتماعية والإنسانية،المجلد 7،العدد،(2021).

23_ محمد در،مجلة الحكمة للدراسات التربوية والنفسية،أهم مناهج وعينات وأدوات البحث العلمي،مؤسسة كنوز الحكمة للنشروالتوزيع،العدد9،الجزائر ،2017.

24_ د.نوفيل حديد_كريبط حنان:امن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة،كلية العلوم الاقتصادية،العلوم التجارية وعلوم التسيير،جامعة الجزائر3،مجلة المؤسسة،العدد ،2004 .

25_د. ولاء السيد عبدالله : إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي بمدارس التعليم الثانوي الصناعي ب ج.م، مجلة الإدارة التربوية ،العدد الثاني عشر –مارس2017 .

<u>المواقع الالكترونية:</u>

26_محمد تيسير،ما هو المنهج الوصفي التحليلي، وأهم خطوات إعداده؟،**المؤسسة العربية للعلوم والنشر والأبحاثhttps://blog.ajsrp.com.**

27_اعمل بزنس، أمن المعلومات: المفهوم، العناصر، التهديدات، ووسائل الحماية،22اكتوبر2022.

https://www.e3melbusiness.com/blog/Information-Security

28_مركز البحث في الإعلام العلمي والتقني، cerist

https://www.cerist.dz/index.php/ar/rechercheetdevelop-/165-divisions-de-recherche-ar/1014-2016-05-02-10-14-49

29_علي خاطر محمد،نظم المعلومات الإدارية،جامعة المجمعة.
https://m.mu.edu.sa/ar/colleges/college-of-science-and-humanities-rumaah/29378

قائمة الملاحق

وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح ورقلة

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

تخصص:اتصال جماهيري والوسائط الجديدة

استمارة مقابلة :

إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية

دراسة ميدانية بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

من إعداد الطالبة:بن قنان أسماء تحت إشراف الأستاذة:جيتي نادية

موظفي الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة. المحترمين:

تشكل هذه المقابلة جزء من دراسة الماستر بهدف معرفة إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية ،نرجو منكم الإجابة عن أسئلة هذه المقابلة ونحيطكم علما أن المعلومات ستعامل بالسرية التامة ولا تستخدم إلا للدراسات العلمية.**مشكورون على التعاون.**

السنة الجامعية:202/2023

أسئلة المقابلة:

المحور الأول: الإجراءات و الوسائل التي تعتمدها الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحماية معلوماتها.

1/ ماهي الإجراءات والوسائل التي تتبعونها لحماية معلومات مؤسستكم؟

1_1)هل تعتمد مؤسستكم على سياسة أمنية خاصة بها؟ماهي هذه السياسة التي تعتمدونها؟

المحور الثاني: الجهة المكلفة بمهمة حماية المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهري ورقلة.

2/ماهي الجهة المكلفة بمهمة حماية المعلومات بمؤسستكم؟

المحور الثالث: البيانات والمعلومات التي تسعى الوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة لحمايتها.

3/ماهي البيانات والمعلومات التي تسعى مؤسستكم لحمايتها؟

3_1)هل تقومون بتحديد المعلومات المهمة والسرية في المؤسسة؟

1_**المحور الرابع:** المخاطر التي تهدد امن المعلومات بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

4/ماهي المخاطر التي تهدد امن المعلومات بمؤسستكم؟

4_1)ماهي التهديدات القادرة على إتلاف نظام معلومات المؤسسة؟

4_2)ماهي الأشكال المختلفة للاعتداءات الالكترونية التي قد تتعرضون اليها؟

المحور الخامس: مدى وعي الموظفين بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة بالأمن المعلومات.

5/مامدى وعي الموظفين بمؤسستكم بضرورة المحافظة على الامن المعلوماتي فيها؟

5_1)هل تقوم مؤسستكم بتوفير برامج توعية أمنية للموظفين؟

5_2)هل تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في الوكالة؟ وهل يطلب من الموظف التوقيع على تهد بعدم الإفصاح عن معلومات حساسة تخص الوكالة كجزء من شروط التوظيف؟

وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح ورقلة

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

تخصص:اتصال جماهيري والوسائط الجديدة

استمارة مقابلة حول:

إستراتيجية الأمن المعلوماتي بالمؤسسات العمومية الجزائرية

دراسة ميدانية بالوكالة الوطنية لتسيير القرض المصغر الفرع الجهوي ورقلة.

من إعداد الطالبة:بن قنان أسماء **تحت إشراف الأستاذة:**جيتي نادية

*بعد التحية والتقدير نضع بين أيدي المبحوثين المحترمين استمارة خاصة ببحث علمي ميداني لتحضير شهادة ماستر حول الموضوع المذكور أعلاه ،كما نحيطكم علما أن هذه الاستمارة تحتوي مجموعة من الأسئلة فالرجاء منكم القراءة المتأنية للأسئلة والإجابة عليها حسب ماهو موجود من معلومات مقدمة في محاور الدراسة ،ونحيطكم علما أن هذه الاستمارة تستعمل فقط لأغراض علمية بحتة.**مشكورون على التعاون.**

السنة الجامعية:202/2023

البيانات الشخصية:

الجنس :ذكر ☐ أنثى ☐

التخصص:.....

الاقدمية: اقل من5سنوات ☐ من6الى10سنوات ☐
اكثرمن10سنوات ☐

المحور الأول :المصادر التي تسهم في تكوين ثقافة الأمن المعلوماتي لدى الموظفين بالوكالة

1/ماهو الأمن المعلوماتي برأيك؟

.....

2/هل تعد المؤسسة محل العمل المصدر الذي تستقون منه معلوماتكم حول الأمن المعلوماتي؟

نعم ☐ لا ☐

1)إذا كانت الإجابة نعم "ماهي" الطرق التي تتبعها مؤسستكم؟

.....

2)إذا كانت الإجابة "لا" ماهي مصادرك الأخرى؟(يمكن اختيار أكثر من إجابة واحدة).

1)مواقع التواصل الاجتماعي ☐

2)مواقع مختصة في إنتاج أنظمة الحماية ☐

3)مواقع الكترونية خاصة بالأمن المعلوماتي ☐

3)تخصصك الجامعي ☐

4)حصص تلفزيونية ☐

5)دورات تدريبية ☐

6)مصادر أخرى ☐

اذكر هذه المصادر الأخرى إن وجدت

.....

3/هل تقوم المؤسسة بتجديد معلوماتكم حول الأمن المعلوماتي

نعم ☐ لا ☐

1)_إذا كانت الإجابة نعم فكيف يكون ذالك:

بصورة دورية منتظمة ☐ عند الضرورة ☐ أخرى ☐

اذكرها إن وجدت:.....

4/هل تلجا لمصادر أخرى لتجديد معلوماتك؟

1)اذكر هذه المصادر:.....

.....

المحور الثاني:امتلاك الموظف لمعلومات حول أساليب وطرق الاختراق الالكترونية

5/هل تمتلك معلومات حول طرق وأساليب الاختراق ؟نعم ☐ لا ☐

6/إذا كانت الإجابة "نعم" من بين طرق الاختراق التالية أيها لديك فكرة عنها؟(يمكن اختيار أكثر من إجابة واحدة).

1)التصيد عبر البريد الالكتروني Phishing Email

2)التصيد عبر الرسائل النصيةSmishing

3)التصيد عبر البرامج الخبيثةMalware_Based Phishing

4)التصيد عبر محركات البحثserhEnging

7/هل تقوم بفتح مواقعك الالكترونية الشخصية في أجهزة المؤسسة؟

نعم ☐ لا ☐

إذا كانت الإجابة نعم:

1)هل تتأكد عند استخدامك للمواقع الالكترونية أنها تستخدم بروتكول"Https"

نعم ☐ لا ☐

8/هل تقوم في العادة بالتثبت من عناوين الوب"URL"في شريط العناوين في المتصفحات (Brozsers)عند استخدامك لهذه المواقع الالكترونية؟

نعم ☐ لا ☐

9/إذا وجدت وسيلة تخزين خارجية(Flash disque ,Carte mémoire.....الخ) مفقودة هل تقوم بتوصيلها بأحد أجهزة المؤسسة؟

نعم ☐ لا ☐

10/من بين البرامج الخبيثةMalware التالية،أيها أنت على دراية بمعناها(يمكن اختيار أكثر من إجابة واحدة)

Virus ☐ Warm ☐ Spyware ☐

Adware ☐

Bot ☐ Trojan horse ☐ Fake ☐ antivirus

Backdoor ☐ Rootkit ☐ ransomewar ☐