



جامعة قاصدي مرباح، ورقلة - الجزائر
كلية العلوم الاقتصادية و التجارية و علوم التسيير
قسم علوم التسيير

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، الطور الثاني
في ميدان : علوم اقتصادية، علوم التسيير وعلوم تجارية
فرع : علوم التسيير، التخصص : تدقيق ومراقبة التسيير

بعنوان :

تقييم مدى مساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظم المعلومات دراسة مقارنة لعينة من المؤسسات

من إعداد الطالب: الطاهر بن عمارة

نوقشت وأجيزت علنا بتاريخ: 13 ماي 2017

أمام اللجنة المكونة من السادة :

(أستاذ محاضر قسم ب- جامعة قاصدي مرباح ورقلة) رئيسا	الدكتور/ نور الدين مزهودة
(أستاذ محاضر قسم ب - جامعة قاصدي مرباح ورقلة) مشرفا ومقررا	الدكتور/ خالد رجم
(أستاذ مساعد- جامعة قاصدي مرباح ورقلة) مناقشا	الاستاذ/ بشير كاوجة

السنة الجامعية : 2016 - 2017



جامعة قاصدي مرباح، ورقلة - الجزائر
كلية العلوم الاقتصادية و التجارية و علوم التسيير
قسم علوم التسيير

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، الطور الثاني
في ميدان : علوم اقتصادية، علوم التسيير وعلوم تجارية
فرع : علوم التسيير، التخصص : تدقيق ومراقبة التسيير

بعنوان :

تقييم مدى مساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظم المعلومات دراسة مقارنة لعينة من المؤسسات

من إعداد الطالب: الطاهر بن عمارة

نوقشت وأجيزت علنا بتاريخ: 13 ماي 2017

أمام اللجنة المكونة من السادة :

(أستاذ محاضر قسم ب- جامعة قاصدي مرباح ورقلة) رئيسا

الدكتور/ نور الدين مزهودة

(أستاذ محاضر قسم ب - جامعة قاصدي مرباح ورقلة) مشرفا ومقررا

الدكتور/ خالد رجم

(أستاذ مساعد- جامعة قاصدي مرباح ورقلة) مناقشا

الاستاذ/بشير كاوجة

السنة الجامعية : 2016 - 2017

الإهداء

أهدي هذا العمل المتواضع إلى أغلى ما في الوجود رجيا من الله أن يحفظهم
هي شمعة تذوب لتنير دروب الآخرين هي زهرة تدبل لتفوح برائحة الياسمين هي
العطاء الذي يفيض بلا حدود هي رمز يجسد الكفاح والخلود نعم أنها

أمي الغالية

إلى قدوتي الأولى ونبراسي الذي ينير دربي.. إلى من علّمني أن أصمد أمام أمواج
البحر الثائرة.. إلى من أعطاني ولم يزل يُعطيني بلا حدود.. إلى من رفعت رأسي عالياً
افتخاراً به

أبي العزيز

أمدّه الله بالصحة والعافية

إلى زوجتي الحبيبة التي أمدتني بالإصرار على مواصلة التعلم
إلى إخوتي و أخواتي الأعمام الذين ساندوني في الوصول إلى ما أنا عليه من ثمرة
النجاح وأتمنى **محمد الأمين ومصطفى** التوفيق في البكالوريا
رغم شقاوتك التي تشقيني وأسئلتك الكثيرة التي تعينني فحبك يا ابنتي **فرح** هو
الذي يحيني وابتسامتك لحزني ينسيني

إلى كل أصدقائي و زملائي في المشوار الدراسي

إلى أساتذتي الكرام

إلى كل من مد لنا يد العون من قريب أو بعيد ولو بكلمة طيبة

إلى كل هؤلاء جميعاً أهدي ثمره هذا العمل المتواضع.

الطاهر بن عمارة

الشكر

" رَبِّ اشْرَحْ لِي صَدْرِي * وَيَسِّرْ لِي أَمْرِي * وَاخْلُ عُنُقَهُ مِّن لِّسَانِي * يَفْقَهُوا قَوْلِي "

سورة طه، الآيات 28 - 25

الشكر والحمد لله ما دامت حيا، والصلاة والسلام على سيدنا محمد نبيا
(صلى الله عليه وسلم)

وأتقدم بجزيل الشكر والامتنان والتقدير إلى الدكتور المشرف خالد رجم على ما بذله من جهد طيب، من خلال إشرافه على هذه المذكرة، والذي لم يبخل علي بوقته وعلمه لإتمام هذا العمل

وكما أتقدم بجزيل الشكر وبأسمى عبارات التقدير والاحترام إلى أختي الفاضلة العزيزة الأستاذة الدكتورة **نوال بن عمارة** على توجيهاتها ومقترحاتها لي في إنجاز هذا البحث

كما لا أنسى شكر الأستاذين اللذين أشرفوا على تحكيم استبيان هذه الدراسة
الدكتور **رشيد مناصرية** الدكتور **الحاج عرابة**

وأتقدم بالشكر كذلك إلى عمال وإطارات جامعة قاصدي مرباح ورقلة وخص
الذكر السيد رئيس قسم علوم التسيير الدكتور **نور الدين مزهودة** على تسييره
المحكم لقسم .

وأتقدم بالشكر إلى إطارات مؤسسات عينة الدراسة أخي زكرياء ، رضوان ، أمين
نجاح على حسن استقبالهم ومساعدتهم لي .

كما أشكر كل من ساعدني من قريب أو من بعيد ولو بكلمة أو دعوة صادقة.

الطاهر بن عمارة

الملخص:

هدفت هذه الدراسة لتعرف على مدى مساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظم المعلومات دراسة مقارنة لعينة من المؤسسات الناشطة في ولاية ورقلة ، ولتحقيق أهداف الدراسة فقد تم استخدام أسلوب تحليل الوصفي ، حيث اعتمدنا في الدراسة على كل من أداة المقابلة و الاستبيان حيث تمثلت عينة الدراسة في ثلاثة مؤسسات اتصالات الجزائر، سونلغاز، ليند غاز بمجموع 228 استبيان موجه إلى مشرفون و مستخدمي النظام لمؤسسات محل الدراسة ، وكانت نسبة الاستجابة 97%، كما تم الاعتماد في التحليل البيانات الاستبانة على برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS وبرنامج الجداول EXCEL و كانت أهم النتائج المتوصل إليها هي : تتعرض المؤسسات إلى عدة مخاطر تهدد أمن نظم المعلومات الإلكترونية، فاعلية السياسات الأمنية و ضوابط للموظفين داخل المؤسسة من شأنه ضمان الحد من المخاطر نظم المعلومات، أن عملية التكوين في مجال الأمن الإلكتروني في المؤسسات به عددة اختلالات ونقائص انطلاقا من تحديد الاحتياجات التكوين في حد ذاته

الكلمات المفتاحية: نظام المعلومات، أمن نظم معلومات، السياسات الأمنية ، مخاطر نظم المعلومات، سونلغاز، اتصالات الجزائر، ليند غاز.

Abstract :

This study aimed to identify the extent of the contribution of the electronic security system to risk reduction Information systems A comparative study of a sample of organizations active in the territory of Ouargla. To achieve the objectives of the study, descriptive and inductive analysis methods were used by collecting information from Arabic and foreign books, periodicals and articles, Distribution of the questionnaire prepared for this study. The sample of the study was composed of three institutions: Algeria Telecom, Sonelgaz, Lindgaz, with a total of 228 questionnaires directed to the information system supervisors and the users of this system for the institutions studied. The results of the analysis were based on the statistical data package on the SPSS program and the EXCEL program. The main findings were: Enterprises are exposed to several risks to the security of electronic information systems, the effectiveness of security policies and controls for employees within the information system from It would ensure the risk reduction of information systems, that the process of training in the field of electronic security in its institutions has returned imbalances and deficiencies based on the identification of the configuration needs in itself

Keywords: Information System, Information Systems Security, Security Policies, Information Systems Risk, Sonelgaz, Algeria Telecom, Lind Gas.

الصفحة	العنوان
III	الإهداء
IV	الشكر
V	الملخص
VI	قائمة المحتويات
VII	قائمة الجداول
VIII	قائمة الأشكال
X	قائمة الاختصارات والرموز
IX	قائمة الملاحق
ب	المقدمة
01	الفصل الأول : الأدبيات النظرية و التطبيقية لمساهمة نظام الأمن الالكتروني في الحد من مخاطر نظام المعلومات
02	تمهيد الفصل الأول
03	المبحث الأول : الإطار النظري لمخاطر نظم المعلومات الالكترونية
23	المبحث الثاني : الدراسات السابقة
27	خلاصة الفصل الأول
28	الفصل الثاني : الدراسة الميدانية لتقييم اثر الأمن الالكتروني على الحد من المخاطر النظم المعلومات
29	تمهيد الفصل الثاني
29	المبحث الأول : الطريقة والأدوات المستخدمة في الدراسة
35	المبحث الثاني : النتائج المتحصل عليها ومناقشتها
82	خلاصة الفصل الثاني
84	الخاتمة
92	المراجع
96	الملاحق
106	الفهرس

قائمة الجداول :

الصفحة	عنوان الجدول	الرقم
07	النظرة الحديثة لنظم المعلومات	1-1
22	أنواع البرامج الخبيثة	2-1
31	الاستثمارات الموزعة على الشركات محل الدراسة	1-2
32	تعريف عينة الدراسة	2-2
35	توزيع موظفي نظام المعلومات لمؤسسة سونلغاز	3-2
35	الأجهزة الكترونية لنظام المعلومات مؤسسة سونلغاز	4-2
37	توزيع موظفي نظام المعلومات لمؤسسة اتصالات الجزائر	5-2
38	الأجهزة الكترونية لنظام المعلومات مؤسسة اتصالات الجزائر	6-2
40	توزيع موظفي نظام المعلومات لمؤسسة ليند غاز	7-2
40	الأجهزة الكترونية لنظام المعلومات مؤسسة ليند غاز	8-2
45	مقياس ليكارت الثلاثي المعتمد في الدراسة	9-2
45	المتوسطات المرجحة والاتجاه الموافق لها	10-2
46	يوضح ثبات استمارة الاستبيان حسب معامل " ألفا كرونباخ "	11-2
46	توزيع حسب الجنس	12-2
48	توزيع حسب الخبرة	13-2
50	توزيع حسب المؤهل العلمي	14-2
52	توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة	15-2
54	توزيع حسب مستوى التدريب الذي يتلقونه مجال امن المعلومات	16-2
56	قياس اتجاه آراء أفراد العينة نحو المحور الثاني مخاطر نظم المعلومات	17-2
64	قياس اتجاه آراء أفراد العينة نحو المحور الثالث نظام الأمن الكتروني	18-2
71	مجموع الاتجاه الآراء الأفراد العينة الدراسة لمحور الثالث	19-2
76	الارتباط سيرمان للارتباط	20-2
80	المقارنة بين السياسات الأمنية المتبعة من المؤسسات عينة الدراسة	21-2
80	المقارنة مدى إمكانية حدوث مخاطر نظام المعلومات بين المؤسسات عينة	22-2

قائمة الأشكال :

الصفحة	عنوان الشكل	الرقم
04	تطور نظام المعلومات	1-1
05	العناصر الأساسية لنظام المعلومات	2-1
07	مستويات نظام المعلومات	3-1
11	عناصر الأمن المعلومات	4-1
21	يوضح النموذج ثلاثي الأبعاد لتصنيف تهديدات نظم المعلومات	5-1
31	توزيع الاستثمارات الموزعة على الشركات محل الدراسة	1-2
34	تقنية خادم/ زيون	2-2
47	توزيع حسب الجنس لمؤسسة سونلغاز	3-2
47	توزيع الأفراد حسب الجنس لمؤسسة اتصالات الجزائر	4-2
48	توزيع حسب الجنس لمؤسسة ليند غاز	5-2
49	توزيع حسب الخبرة لمؤسسة سونلغاز	6-2
49	توزيع الأفراد حسب الخبرة لمؤسسة اتصالات الجزائر	7-2
50	تطور نظام المعلومات توزيع حسب الخبرة لمؤسسة ليند غاز	8-2
51	توزيع حسب المؤهل العلمي لمؤسسة سونلغاز	9-2
51	توزيع الأفراد حسب المؤهل لمؤسسة اتصالات الجزائر	10-2
52	توزيع حسب المؤهل العلمي لمؤسسة ليند غاز	11-2
53	عناصر الأمن المعلومات توزيع حسب مدى استخدام المؤسسة لنظم	12-2
53	توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة لمؤسسة	13-2
54	توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة لمؤسسة	14-2
55	توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات	15-2
55	توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات	16-2
56	توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات	17-2

قائمة الملاحق:


الرقم	عنوان الملحق
01	أسئلة المقابلة
02	استمارة الاستبيان
03	واجهة نظام المالي ومحاسبي سونلغاز
04	واجهة تقنية الاتصال للبريد الداخلي المحلي سونلغاز
05	واجهة تقنية الاتصال للبريد الداخلي الواسع سونلغاز
06	نافذة من البرنامج اتصالات الجزائر
07	نافذة الدخول للبرنامج اتصالات الجزائر
08	قائمة البرنامج اتصالات الجزائر
09	لائحة تنظيمية للأمن الإلكتروني للمؤسسة ليند غاز

قائمة الرموز:

الاختصار	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
SPSS	Statistical Package for Social Sciences	الحزمة الإحصائية للعلوم الاجتماعية
ISACA	Society for the Review and Control of Information Systems	جمعية مراجعة ومراقبة نظم المعلومات
RMS	Multi Service Network	شبكة متعددة الخدمات
VPN	Vitual Private Network	الشبكة المحلية الافتراضية
IP	Internet Protocol	بروتوكول أنترنت
TCP	Transmission Control Protocol	بروتوكول التحكم بالنقل
VPN	Vitual Private Network	الشبكة المحلية الافتراضية
ELIT	El Djazair Information Technology	الجزائر انفورماسيو تكنولوجي
HDSL	High bit rate digital subscriber line	خط رقمي بتدفق ثنائي مضاعف
NOVA	Système d'information Ressources humaines	نظام معلومات موارد بشرية
LAN	Local Area Networks	الشبكة المحلية للاتصالات
WAN	Wide Aera Networks	الشبكة الواسعة للاتصالات
SGC	Customer Information Management System.	نظام معلومات تسيير الزبائن.
HISSAB	Accounting Information System	نظام معلومات مالي محاسبي
ERP	Resource Planning System	نظام تخطيط موارد



المقدمة



توطئة:

يتميز العصر الحديث بتطور كبير في مجال تكنولوجيا المعلومات والاتصال ، حيث أدى هذا التطور إلى ازدياد حجم المعلومات التي يجب أن تعالج وتخزن وتقدم للنظام بشكل كبير ، مما عقد عملية التحكم بها والسيطرة عليها ، وبالمقابل هذا التقدم التكنولوجي الكبير قد يحمل بين طياته الكثير من المخاطر الهامة المتعلقة بنظم المعلومات الذي يجب أن يتضمن وسائل وضوابط رقابية على البيانات حتى يتم تقديم تقارير تشمل معلومات موثوق بها ، لذا سعت المؤسسات باختلاف أحجامها وأنواعها إلى مواكبة التطورات التكنولوجية ووسائل الحماية وأمن المعلومات والبيانات ذات الصلة للحد من السرقة والاختراق من خلال الإدارة السلمية لأمن معلوماتها وشبكات اتصالاتها.

كما أن استخدام تكنولوجيا المعلومات والاتصال وفر الكثير من الوقت والجهد للعاملين ، إلى أنه أدى إلى زيادة مخاطر أنظمة المعلومات في ظل الانفتاح على الاقتصاد العالمي ، من هنا كان على المؤسسات أن تشدد من إجراءاتها الأمنية لحماية أنظمتها المعلوماتية ، و من هذا المنطلق سعت العديد من الشركات الوطنية، إلى تصميم وبناء نظام معلومات إلكتروني، مستهدفة من خلاله توفير نظام أمن الكتروني لما يميز هذا النظام من بنية تحتية، تتمثل في الحواسيب وأجهزة شبكات الاتصالات الإلكترونية وقواعد البيانات، التي تتميز بالسرعة الفائقة في المعالجة والاسترجاع للمعلومات والقدرة الهائلة على تخزين المعلومات، بما يحقق السيطرة على الكم الهائل من المعلومات الضرورية، ضمان وصولها موثقة وصحيحة إلى كافة المستويات الإدارية بالشكل الملائم وفي الوقت المناسب.

01. الإشكالية :

ويمكن صياغة إشكالية الدراسة كما يلي:

ما مدى فعالية نظام الأمن الالكتروني في الحد من مخاطر نظم المعلومات في عينة الدراسة؟

02. الأسئلة الفرعية :

1. ما مدى كفاءة مكونات نظام المعلومات الالكتروني في المؤسسات محل الدراسة؟
2. ما مدى فعالية نظام الأمن الالكتروني في المؤسسات محل الدراسة؟
3. ما هي المخاطر المحيطة بنظم المعلومات الكترونية في المؤسسات محل الدراسة؟
4. إلى أي مدى يساهم نظام الأمن الالكتروني في الحد من مخاطر نظام المعلومات في المؤسسات محل الدراسة؟

03. فرضيات الدراسة :

من خلال الإشكالية يمكن صياغة الفرضية التالية :

1. تتميز نظم المعلومات في عينة الدراسة بالكفاءة من خلال المكونات (المادية و البرمجيات).
2. لدى المؤسسات محل الدراسة نظام امن الكتروني يشمل كل عناصر الأمن الالكتروني لحماية أنظمتها من كل أنواع الاختراق.
3. تحيط بأنظمة معلومات المؤسسات محل الدراسة العديد من المخاطر نلخصها في:

✓ مخاطر تتعلق بإدخال البيانات

✓ مخاطر تتعلق بالتشغيل

✓ مخاطر تتعلق بالمرحجات

✓ مخاطر تتعلق بالبيئة

4. هناك تفوت في إمكانية نظام الأمن الالكتروني في الحد من المخاطر بين المؤسسات محل الدراسة، و ترجع أسباب حدوث المخاطر التي تهدد نظم المعلومات في المؤسسة :

✓ أسباب تتعلق بموظفي المؤسسة نتيجة قلة الخبرة والوعي الأمن الالكتروني .

✓ أسباب تتعلق بإدارة المؤسسة نتيجة لعدم سياسات واضحة والإجراءات الرقابية المطبقة .

4. أهداف الدراسة :

بناء على ما تم توضيحه في الإشكالية وأهميتها ، فإن الدراسة تهدف بصفة أساسية إلى تحقيق النقاط التالية :

1. التعرف على طبيعة المخاطر التي تهدد أمن نظم المعلومات؛
2. تحديد اثر السياسات والإجراءات على أمن المعلومات في مؤسسات اتصالات الجزائر وسونلغاز وليندغاز ؛
3. إبراز درجة الارتباط بين الأمن الالكتروني ومخاطر نظم المعلومات في مؤسسات اتصالات الجزائر وسونلغاز و ليندغاز ؛
4. إبراز أثر مخاطر نظم المعلومات على سيرورة الأمن الالكتروني في المؤسسات الاقتصادية ؛
5. مقارنة حالة الدراسة مع الجانب النظري للدراسة ؛
6. إظهار الصعوبات والمعوقات التي تواجه المؤسسات في ظل بيئة الالكترونية.

05. منهجية الدراسة والأدوات المستخدمة:

بغية الوصول إلى الأهداف المرجوة وللإجابة على إشكالية الدراسة فإننا اتبعنا المنهج الوصفي التحليلي الموافق للدراسة النظرية من خلال دراسة المفاهيم المتعلقة بأمن نظام المعلومات ومخاطره، وكذا أهم الدراسات ذات الصلة بالموضوع لنتمكن من خلالها بتدعيم الأسس النظرية، أما بالنسبة للجانب التطبيقي فقد اعتمدنا على منهج دراسة الحالة من خلال تحليل واقع نظام الأمن الإلكتروني في مؤسسات اتصالات الجزائر وسونلغاز وليندغاز ، و إجراء مقابلة مع الإطارات المختصة لتشخيص مخاطر نظام المعلومات الإلكتروني في المؤسسات عينة الدراسة ، كما استخدمنا أداة الاستبيان بهدف التعرف على نجاعة نظام الأمن الإلكتروني للحد من مخاطر نظم المعلومات ، بهدف تحقيق الربط بين الإطار النظري للدراسة والواقع التطبيقي لها.

06. مبررات اختيار موضوع الدراسة :

وقع اختيار الباحث لهذا الموضوع الذي يتمحور حول تقييم مدى مساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظم المعلومات، من خلال إبراز طبيعة المخاطر التي تهدد أمن نظم المعلومات ، لسببين أساسيين هما :

✓ مبررات موضوعية :

- ✚ حدثت موضوع الدراسة حيث يعتبر موضوع أمن نظم المعلومات من الموضوعات الحديثة الجديدة بالبحث؛
- ✚ إلزامية مواكبة نظم المعلومات في المؤسسات الجزائرية لمستجدات تكنولوجيا المعلومات والاتصال؛
- ✚ الصعوبات التي تعاني منها المؤسسات الجزائرية في جانب تطوير امن نظام معلوماتها ؛
- ✚ موضوع الدراسة يدخل ضمن تخصص الباحث.

✓ مبررات ذاتية :

- ✚ تركيز اهتمامات الباحث في مجال أنظمة المعلومات؛
- ✚ قناعة الباحث بأهمية نجاعة نظام الأمن الإلكتروني للحد من مخاطر نظم المعلومات للمؤسسات الجزائرية.

07. أهمية الدراسة :

تكتسب هذه الدراسة أهميتها أساسا من أهمية استخدام أنظمة المعلومات، والتي تساهم في خدمة العديد من الأفراد والمؤسسات في المجتمع ، إلا أن سوء استخدام إجراءات أمن المعلومات تفقد طبيعتها إذا تم تفسيرها بطريقة خاطئة من قبل العاملين، كما أن المورد البشري هو الركيزة الأساسية لتطبيق وإنجاح سياسة الأمن الإلكتروني والحد من مخاطر نظم المعلومات ، وكذا العمل على استقرار آراء مسؤولي أنظمة المعلومات بمؤسسات اتصالات الجزائر وسونلغاز وليندغاز لنقاط وعناصر البحث المختلفة ، هو محاولة لربط الواقع العملي بالدراسة النظرية .

08. حدود الدراسة:

❖ الحدود الزمنية :

تمت الدراسة الميدانية خلال الفترة الممتدة من فيفري 2017 إلى غاية افريل 2017.

❖ الحدود المكانية :

تم إجراء الدراسة الميدانية في مؤسسة سونلغاز مديرية التوزيع بورقلة ، ومؤسسة اتصالات الجزائر بورقلة ومؤسسة ليندغاز وحدة ورقلة.



الفصل الأول: الأدبيات النظرية والتطبيقية لمساهمة نظام

الأمن الإلكتروني في الحد من مخاطر نظام المعلومات



تمهيد:

تعد المعلومات اليوم مورداً مهماً ورئيسياً من موارد المنظمة؛ ذلك أنها تشكل عاملاً هاماً لنجاح المنظمة في تحقيق رسالتها وأهدافها، خاصة في ظل عالم يتميز بدرجة عالية من التعقيد والتغيير، نتيجة التطورات التكنولوجية المتسارعة؛ وظهور الشركات متعددة الجنسيات، وانتشار مفاهيم الخصوصية والعوامة، أصبحت المعلومة سلاحاً تنافسياً، ومورداً استراتيجياً يتوقف عليه نجاح المنظمة أو فشلها.

وعلى الرغم من ضرورة توافر المعلومات لأي منظمة، إلا أن ذلك ليس كافياً لحل المشكلات التي قد تواجهها، فالمعلومات يجب أن توضع في نظام يسهل عملية الحصول عليها في الوقت المناسب والكافي، حيث شهدت المنظمات العامة والخاصة نقلة كبيرة في أنظمة المعلومات، تمثلت باستخدام الحاسب وقواعد البيانات وشبكات الاتصال، بالإضافة للوسائل التكنولوجية الأخرى التي ساهمت في وجود نظام المعلومات والأمن الالكتروني من أجل الحد من مخاطر التي تهدد هذه المنظمات ومن خلال ما سبق سيتم تقسيم الفصل الأول إلى مبحثين حيث تناول في المبحث الأول إلى ثلاثة مطالب عمومية حول نظم المعلومات والأمن الكتروني وخصصنا المطلب الثاني بالمخاطر وتهديدات المحيطة بالنظام المعلومات .

وكما تناول المبحث الثاني الدراسات السابقة وقمنا بتقسيم بنفس طريقة المبحث السابق إلى ثلاثة مطالب خصصنا المطلب الأول الدراسات السابقة باللغة العربية أم المطلب الثاني الدراسات السابقة باللغة الأجنبية وقمنا بمقارنة الدراسات السابقة بالدراسة الحالية وما يميزها على غيرها في المطلب الثالث .

المبحث الأول: الإطار النظري لمخاطر نظم المعلومات الالكترونية

المطلب الأول: عموميات حول نظام المعلومات:

وقد أصبحت نظم المعلومات عنصرا أساسيا في المنشأة يعتمد عليه في شتى المجالات لدعم أنشطتها من أجل تحقيق أهدافها المنشودة سواء كانت تلك الأهداف تسعى إلى تحقيق الربح أو لا تسعى إلى تحقيق الربح؟

تعتبر نظم المعلومات المصدر الرئيسي للمعلومة اللازمة لاتخاذ القرارات المناسبة التي تساعد على أداء وظائفها بالطريقة الصحيحة والمثلى والوصول إلى الأهداف المطلوبة بأفضل الطرق وأمثلها وأحسنها.

الفرع الأول: ماهية نظام المعلومات :

أولا: التعريف الأول:

"هو مجموعة من الإجراءات التي تتفاعل مع بعضها البعض بهدف معالجة البيانات وتحويلها بهدف استخدامها في العملية صنع القرار إن المعلومات هي بيانات تمت معالجتها بشكل يسمح باستخدامها والاستفادة منها حيث أصبحت ذات معنى وفائدة , فالمعلومات هي البيانات التي خضعت للمعالجة والتحليل والتفسير, بهدف استخراج المقارنات والمؤشرات والعلاقات التي تربط الحقائق والأفكار والظواهر مع بعضها البعض"¹.

ثانيا: التعريف الثاني:

" نظام المعلومات بأنه مجموعة من العاملين والإجراءات والموارد، التي تقوم بتجميع البيانات ومعالجتها ونقلها لتتحول لمعلومات مفيدة وإيصالها إلى المستخدمين بالشكل الملائم والوقت المناسب من أجل مساعدتهم في أداء الوظائف المسندة إليهم"².

ثالثا: التعريف الثالث:

"An information system can be defined technic 63 ally as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting décision making ,coordination, and control, information systems may also help managers and workers analyze problèmes, visualize complex subjects"³

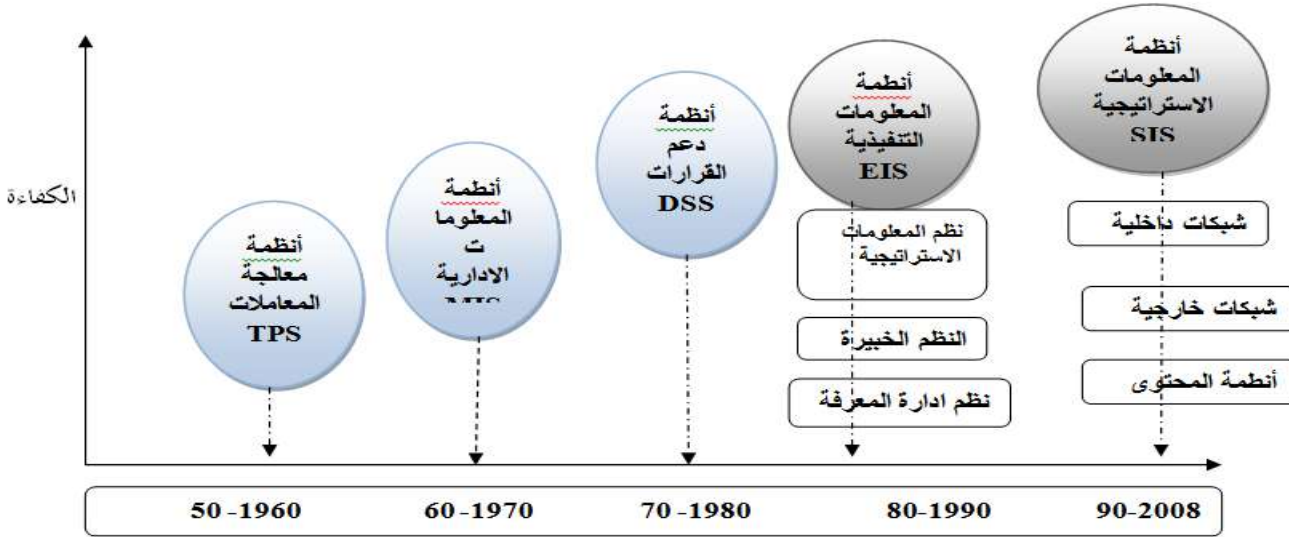
¹ - أحمد فتحي الحيت، مبادئ الإدارة الالكترونية، دار الخامد للنشر والتوزيع، عمان، 2015، صفحة 114

² Oihab Allal-Chérif et Olivier Dupouet, « Optimisez votre Système d'Information « vers la PME numérique en réseau » », Afnor,Saint-Denis, France,2014, p :1

³ laudon & laudon-management information systems-the digital firm , idition9, Pearson Education, USA,2006, page50

يمكن تعريف نظام معلومات فنيا كمجموعة من المكونات المترابطة تهدف إلى جمع ومعالجة وتخزين وتوزيع المعلومات لدعم القرار والتحكم في المنظمة وبالإضافة إلى دعم عملية صنع القرار، التنسيق، والسيطرة، فان نظم المعلومات تساعد أيضا الإدارة العليا على تحليل المشاكل و الموضوعات المعقدة.

الشكل رقم(1-1): تطور نظام المعلومات



المصدر: رجم خالد، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2017 ص 49

من الشكل أعلاه تتضح فكرة جوهرية في نظام المعلومات، وهي أن ظهوره كان بهدف تقديم الدعم والمساندة لإدارة المنظمات في مختلف المستويات، لكن التطور التكنولوجي في ميدان الحاسوب والبرمجيات خلال الفترة الممتدة من 1970 إلى 1990، وظهور تقنيات الإعلام والاتصال TIC فتحت مجالا واسعا لاستخدامات متطورة له.

كما نجد إن نظم معالجة المعاملات هي أول نظم المعلومات التي ظهرت في المؤسسة لدعم المستوى التشغيلي ثم ظهرت نظم المعلومات الإدارية التي تدعم وظائف المؤسسة، بعدها ظهرت نظم دعم القرار التي تساعد على اتخاذ القرارات في ظل عدم التأكد، بالإضافة إلى النظم التنفيذية، وأخرها نظم المعلومات لإستراتيجية كما لا ننسى آخر تطبيقات أنظمة المعلومات في المؤسسة وهي نظام تخطيط موارد المؤسسة ERP .

الفرع الثاني: عناصر نظام المعلومات

يتكون أي نظام للمعلومات في أي مؤسسة من مجموعة من العناصر، وهذه العناصر لا تعدو أن تكون المدخلات بأشكالها المتنوعة، المعالجة أو التشغيل، ثم المخرجات على الصورة المخطط لها ثم التغذية المرتدة والرقابة عليها والبيئة الخارجية المحيطة والمؤثرة في المؤسسة، وتتمثل في التالي:

أولاً: المدخلات: تتمثل في سلسلة البيانات التي تنساب من قنوات الاتصال المختلفة من المصادر الداخلية والمصادر الخارجية أو من النظام ذاته عندما يعتمد جزء من مخرجاته كمدخلات جديدة لتغذية النظام⁴.

ثانياً: المعالجة: تتم معالجة البيانات المدخلة بإجراء عدد من العمليات لإنتاج المخرجات المعينة المحتاج إليها⁵.

ثالثاً: المخرجات: تتحول المدخلات بفعل عمليات المعالجة إلى المخرجات التي تطرح في البيئة المحيطة أو تستخدم كمدخلات جديدة للنظام نفسه، والتي تكون على نوعين حصراً في جميع أنواع الأنظمة وهما المادة فقط أو المعلومات فقط أو كليهما معا.

رابعاً: التغذية العكسية: هي سريان وتدفق المعلومات من وإلى النظام بعد تقييم العمليات المنفذة وأخذها بعين الاعتبار في ضوء القرارات والعمليات المستقبلية، وهي في الواقع دليل للأداء المستقبلي وتقوم بتصحيح النظام من خلال ضوابط وتعديلات لازمة للتخلص من الأخطاء ورفع كفاءة الأداء للنظام. تحقيق الأهداف التي يرمي النظام تحقيقها خدمة للشركة ككل

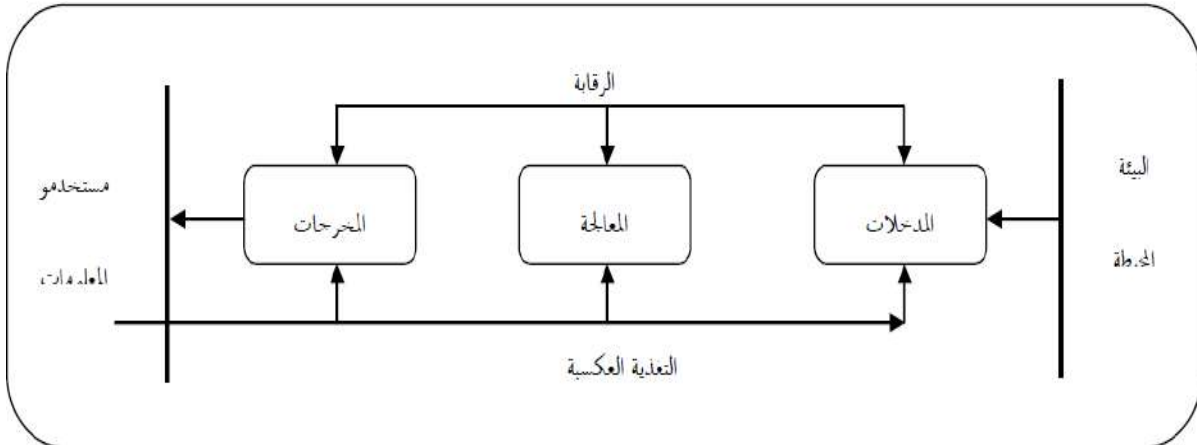
خامساً: الرقابة: هي مقياس الأداء وضبط العمليات المؤدية إلى الهدف المرجو، وهي محصلة معرفة سبق تحديدها عن آلية عمل النظام وتشمل الرقابة قياس وتقييم مسار المدخلات، العمليات والمخرجات، للتأكد بأن النظام يؤدي وظائفه بصورة متماسية مع الأهداف والمخطط الموضوع، فإذا كانت هناك أي انحرافات فإنه يجري القيام بالتعديلات اللازمة على المدخلات والعمليات والمعالجة وصولاً لتصحيح المسار نحو الأهداف الموضوع.

سادساً: البيئة: تتأثر المؤسسة بالبيئة المحيطة بها، وتصدر مخرجاتها أيضاً إلى هذه البيئة بعد تشغيلها، مما يعني وجود علاقة تبادلية وثيقة بين المؤسسة والبيئة المحيطة يؤثر كل منهما في الآخر سلباً أو إيجاباً ويزداد هذا التأثير إذا كانت البيئة محكومة ومقيدة مثل النظم الاقتصادية والسياسية الموجهة أو المغلقة وفق الشكل الآتي:

⁴ محمد آل فرج الطائي، الموسوعة الكاملة في نظم المعلومات الإدارية الحاسوبية، دار زهران، الأردن، 2002، ص: 44

⁵ أبو بكر محمود الهوش، نظم وشبكات المعلومات، مؤسسة الثقافة الجامعية، مصر، 2007، ص: 95

الشكل رقم (1-2): العناصر الأساسية لنظام المعلومات



المصدر: عبد الرزاق محمد قاسم، تحليل وتصميم نظم المعلومات المحاسبية، دار الثقافة، دمشق، 2009، ص 16.

من خلال الشكل السابق يتبين سير المعلومة بدءاً من مستخدم المعلومات تم تحويلها إلى مدخلة، ثم معالجتها تم تحويلها إلى مخرجات، كل هذا من خلال تواجد رقابة عبر كل مراحل .

الفرع الثالث: أنواع نظم معلومات حسب مستويات التسيير

إن نظم المعلومات تتوزع حسب المستويات التنظيمية بالمؤسسة حيث يمكن تصنيفها ابتداءً من المستوى الأدنى وصعوداً إلى المستوى الأعلى كالآتي:⁶

أولاً: المستوى الاستراتيجي (Strategic Level Systems):

Information systems that support the long-range planning activities of senior management.

نظم المستوى الاستراتيجي، التي تمكن المديرين في الإدارة العليا من القيام بالنشاطات ذات البعد الاستراتيجي، وتسمح لهم بتحديد الأهداف طويلة الأجل، واختيار الوسائل الضرورية لتحقيقها فالهدف من هذه النظم هو إحداث التوافق بين التغيرات التي تحدث في البيئة الخارجية للمؤسسة مقارنة بقدرتها الحالية والمستقبلية وتساعد هذه النظم في الإجابة على عدة تساؤلات منها :

كيف ستكون مستويات العمالة في الخمس سنوات المقبلة؟ ما هو اتجاه تكاليف الصناعة مستقبلاً؟ ما هي المنتجات التي يجب تقديمها خلال الخمس سنوات المقبلة؟

بالإضافة إلى دراسة الوضع الاستراتيجي، تخطيط الأرباح، التنبؤ بالمبيعات لخمس سنوات، التخطيط الاستراتيجي) ...؛

ثانياً : المستوى الإداري (Management level Systems):

Information systems that support monitoring, controlling, decision making, and administrative activities of middle managers.

⁶ laudon & laudon-management information systems-the digital firm , idition9, Pearson Education, USA,2006, page25

أما نظم المستوى الإداري، فهي تعمل على مساندة مسؤولي الأنشطة في اتخاذ القرارات شبه الهيكلية وتسيير الأنشطة في الإدارة الوسطى، كما تخدم تخطيط الوظائف عن طريق تقديم ملخص روتيني يهدف إلى تحقيق السرعة في إنجاز التقارير المطلوبة، والتساؤل الرئيسي الذي تحاول هذه النظم الإجابة عليه هو :

ما هو وضع المؤسسة مقارنة بالتوقعات ؟ وما هي أهدافها التشغيلية ؟ كما يشتمل على (إدارة المبيعات، تحليل مبيعات السوق، تخطيط الإنتاج، تسيير المخزون، تسيير الموازنة السنوية)... حيث يتم في هذا المستوى استعمال المعلومات لاتخاذ القرارات القصيرة الأجل؛

ثالثا : المستوى التشغيلي (Operational level systems):

Information systems that monitor the elementary activities and transaction of the organization.

فنظم المستوى التشغيلي تعمل على دعم النشاطات الروتينية المتكررة ومتابعة سير المعاملات داخل المؤسسة والمرتبطة بالوظائف الأساسية من تسويق ومبيعات، إنتاج وتصنيع، مالية ومحاسبة، موارد بشرية وهي تجيب على الأسئلة المختلفة المتعلقة بهذه الوظائف.

الجدول رقم(1-1) : النظرة الحديثة لنظم المعلومات

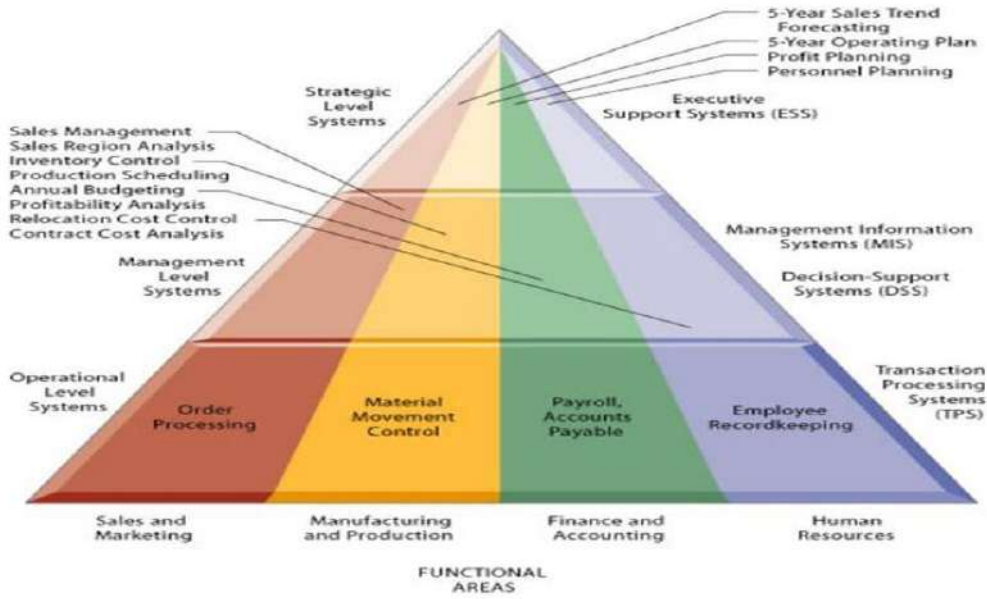
النظرة التقليدية	النظرة الإستراتيجية
وظيفة إدارة نظام المعلومات هي مركز تكاليف.	نظام المعلومات عنصر من عناصر سلسلة القيمة.
تكنولوجيا المعلومات والاتصال هي وسيلة.	نظام المعلومات هو أصل من أصول المؤسسة.
تكنولوجيا المعلومات والاتصال لها أثر ودور وظيفي وتشغيلي	نظام المعلومات له وظيفة الدعم الاستراتيجي.
تستغل تكنولوجيا المعلومات والاتصال في كل وظيفة على حدا.	نظام المعلومات عبارة عن نظام مدمج و متكامل و يشار في تسييره جميع الأطراف.
تكنولوجيا المعلومات والاتصال ميدان مختكر من طرف مهندسي الإعلام الآلي فقط.	نظام المعلومات ميدان متعدد وليس مخصص لفئة معينة حيث يستخدم و يسير من طرف المسيرين +مهندسي الإعلام الآلي.

المصدر : رجم خالد، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم

الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2017 ص53

ما نستنتجه من الشكل أعلاه أن النظرة لنظم المعلومات قد تطورة بشكل كبير من نظرة تقليدية وظيفية روتينية إلى نظرة إستراتيجية حيث أصبحت نظم المعلومات كوسيلة لتحقيق الميزة التنافسية و تحقيق الأداء المطلوب لكن هذا يتوقف دائما على مدى الاستغلال الأمثل للنظام و مدى توافق النظام مع إستراتيجية المؤسسة.

الشكل رقم (1-3): أنواع نظم المعلومات حسب مستويات التسيير



Source :laudon & laudon-management information systems-the digital firm , idition9, Pearson Education, USA,2006, p26

الفرع الرابع: أهداف نظام معلومات: تتلخص هذه أهداف في الآتي:⁷

أولاً: تزويد الإدارة العليا بالمعلومات : تحتاج الإدارة في جميع أعمالها إلى المزيد من المعلومات، بحيث يعمل النظام على مد الإدارة العليا بمعلومات عن الفرص والتهديدات النابعة من البيئة الخارجية، وكذلك عن مؤشرات الأداء داخل المؤسسة وهو ما يمكن الإدارة من زيادة القيمة المضافة.

ثانياً: تحديد المسؤولية : تساعد نظم المعلومات في تحديد أدوار الأفراد والأقسام بالمؤسسة وبالتالي تحديد مسؤولية هؤلاء، وتحديد المسؤولية فإنه يمكن محاسبة المقصرين والتعرف على المهملين.

ثالثاً: تخفيض عدد المشاكل : لعل الهدف الحقيقي من التفكير في نظام جديد هو التخلص من المشاكل الموجودة في ظل النظام الحالي، بيد أنه عملياً من غير الممكن التخلص من كل المشاكل ولكن فقط تخفيض عددها وتخفيض حجمها كلما أمكن ذلك.

رابعاً: تنظيم الإجراءات: وهذه الوظيفة للنظام مستمدة من الاسم " نظام " أي شيء مخطط ومحدد ومرتب وفي غيبة النظام فإن الغلبة تكون للفوضى والعشوائية، والمؤسسة تتوقع من النظام الجيد تقنين الإجراءات وسد الثغرات في سير خطط العمل الحالية.

⁷ - محمد الصبري، نظم المعلومات الإدارية ، طبعة الأولى، مؤسسة حورس الدولية، الإسكندرية، 2005، ص 186-188

خامسا: السيطرة على الموارد المتاحة : الموارد المتاحة قد تكون مادية كأجهزة ومعدات، أو بشرية كالعاملين والعملاء أو معنوية كبيانات موجودة أو يمكن الحصول عليها، إلا أن هذه الموارد التي قد تكون السيطرة عليها عملاً في منتهى الأهمية، للاستفادة منها استفادة قصوى .

فعلى سبيل المثال يمكن للمؤسسة أن تحصر عدد وتخصصات العاملين، لتعيد توزيع أدوارهم ووظائفهم ما يكفل الاستفادة منهم في زيادة الإنتاج دونما الحاجة لتعيين أي عامل إضافي.

سادسا: ضمان انسياب العمل: من وظائف النظام أن يؤدي إلى التنسيق والانسجام بين النظم الفرعية بما يكفل انسياب العمل والتخلص من الاختناقات الموجودة، ففي مؤسسة يتم العمل على مراحل يجب أن يعمل النظام على توزيع الأدوار والطاقات، بما لا يخلق تكديساً في مرحلة ما فتتعطل السلسلة.

المطلب الثاني: أمن نظام المعلومات :

تشكل المعلومات للمنظمات البنية التحتية التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بمجازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وأبعادها عن الاستخدام غير المشروع لها.

وستتناول في هذا المطلب الحديث حول تعريف الأمن المعلومات، مفهوم أمن نظم المعلومات، عناصر أمن نظم المعلومات، الغرض من تحقيق الأمن، تصميم النظام الأمني.

الفرع الأول: ماهية أمن المعلومات

تعريف الأول: "يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وإن تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة."⁸

تعريف الثاني: " هو عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونياً عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمؤمنين وأي شخص آخر ممكن أن يكون معرضاً لمخاطر الاختراق"

الفرع الثاني:عناصر أمن المعلومات:

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنف تلك العناصر إلى خمسة عناصر وهي:

⁸ - رجم خالد ، أمن المعلومات ، محاضرات مقياس مراجعة نظام المعلومات سنة أولى ماستر تدقيق ومراقبة التسيير ، جامعة ورقلة 2015، -2016 ، ص 08

أولاً: السرية أو الموثوقية (Confidentiality): وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها.

ثانياً: التعرف أو التحقق من هوية الشخصية (Authentication): وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم، وتوضح مؤسسة (RSA) لأمن المعلومات RSA Security Inc ثلاث طرق للتحقق من الشخصية وهي:

- 1- عن طريق شيء يعرفه الشخص مثل كلمة المرور .
- 2- عن طريق شيء يملكه مثل رسالة الشيفرة (Token) : وهي عبارة عن كود يقوم بإدخاله المستخدم للحاسوب للحياسة على صلاحيات التشغيل أو الشهادة الإلكترونية.
- 3- عن طريق شيء يتصف به الشخص من الصفات الفيزيائية مثل بصمة الإصبع أو المسح الشبكي أو نبرة الصوت، وكل طريقة لها إيجابياتها وسلبياتها، وتنصح مؤسسة RSA باستخدام طريقتين مع بعضهما البعض من هذه الطرق الثلاثة.

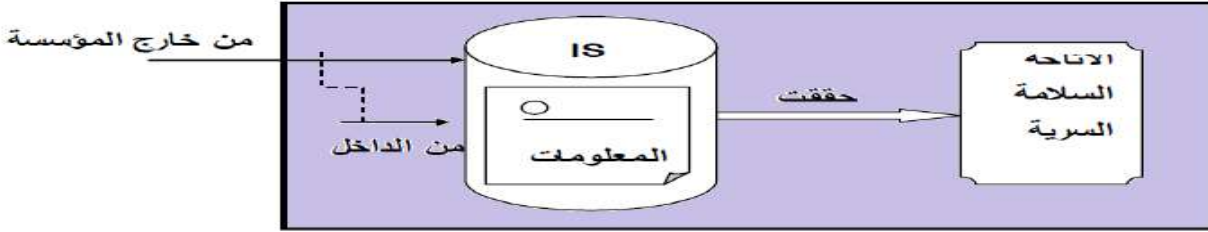
ثالثاً: سلامة المحتوى (Integrity): وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخلياً في المشروع أو خارجياً من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالباً بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات.

رابعاً: استمرارية توفر المعلومات أو الخدمة (Availability): وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العشبية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة.

خامساً: عدم الإنكار (No repudiation): ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في

وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونياً يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية⁹.

الشكل رقم (1-4): عناصر الأمن المعلومات



المصدر: أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية، أطروحة ماجستير، كلية التجارة، غزة، 2013
ص 47

الفرع الثالث: متطلبات أمن نظم المعلومات :

تعتبر مسألة حماية أمن نظم المعلومات من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات¹⁰

- ✓ وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المنشأة.
- ✓ يجب على الإدارة العليا في المنشأة دعم أمن نظم المعلومات لديها.
- ✓ يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين.
- ✓ تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.
- ✓ تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.
- ✓ الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن.
- ✓ تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.
- ✓ تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

الفرع الرابع: تصميم نظام الأمن:

من منطلق أن الإخلال بالأمن قد يكون مدبراً أو قد يكون حادثة غير مدبرة، فعلى سبيل المثال الحريق كإحدى الحوادث الممكنة يمكن أن يحدث نتيجة ماس كهربائي فهو بالتالي حادثة غير متعمدة، أو أن ينتج بسبب أشخاص يتعمدون التخريب.

⁹ - حرية شعبان محمد الشريف، مخاطر نظم المعلومات المحاسبية الإلكترونية "دراسة تطبيقية على المصارف العاملة في قطاع غزة"، مذكرة ماجستير منشورة، كلية التجارة بالجامعة الإسلامية بغزة، 2006

¹⁰ - أمل إبراهيم أبو رحمة، نظام معلومات الموارد البشرية وأرها على فاعلية إدارة شؤون الموظفين في فلسطين، مذكرة ماجستير، إدارة الأعمال، غزة 2005 ص 58

وعليه يتبين أن تصميم نظام الأمن من الموضوعات المعقدة، و مرورا بالكثير من الاجتهادات التي وضعت تصاميم وخطوات واعتبارات عدة قد حدد خطوات أو مراحل أساسية لهذا التصميم تتخلص في الآتي¹¹:

أولاً: الوقاية : وتعتبر من أمثل المفاهيم النظرية ولكن يصعب تنفيذها وذلك لكثرة تكاليف الاحتياطات الخاصة بها ولكنها رغم ذلك تعتبر أهم مراحل تصميم نظام الأمن.

ثانياً: الكشف: وهو يوجد عديد من الوقاية في نظام الأمن، فمثلاً قد يوفر النظام الوقاية ضد الدخول غير المسموح به كما يسجل محاولات الدخول الفاشلة لكشف نوع النشاطات التخريبية وكذلك الأشخاص القائمين بهذه النشاطات.

ثالثاً: الردع : يجب توفير الردع المناسب للنشاطات التخريبية لأن ذلك يؤدي إلى خوف المخربين من اكتشاف أمرهم ومحاسبتهم.

رابعاً: استعادة الأجزاء المفقودة: يجب اتخاذ الإجراءات اللازمة لسرعة استعادة الأجزاء المفقودة من النظام، وذلك باستخدام النسخ الاحتياطي.

خامساً: الإبطال وإعادة الإنتاج: عندما تفشل جميع إجراءات الأمن في التغلب على تهديد معين فإن الوسيلة الوحيدة الباقية هي إعادة تصميم النظام مرة أخرى مع اتخاذ الإجراءات الأمنية الجديدة التي تعمل على منع مثل هذا التهديد.

المطلب الثاني: مخاطر وتهديدات نظام المعلومات :

توجد كثير من التحديات التي تؤثر على الأداء السليم لوظائف نظم المعلومات في ظل التطورات التكنولوجية المتسارعة، أو لمشكلات الفنية المتزايدة، أو الأحداث البيئية المتغيرة ، أو لضعف البشري، وعدم ملائمة المؤسسات الاجتماعية والسياسية والاقتصادية الراهنة للمتغيرات المتلاحقة، الخ ...، وتنبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية، كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم تحقيق الغايات الأمنية.

وقد تنشأ أخطاء النظام من سوء استخدام الأجهزة والبرمجيات بما تحدثه من الأخطاء الكامنة، أو التحميل الزائد أو المشكلات التشغيلية وغير ذلك، والعوامل الفنية التي تؤدي لفشل نظم المعلومات عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان أو تتغير على الدوام و قد تنتج الأعطال من أعطال كبيرة تؤدي إلى توقف العمل أو إبطاء العمل بصفة دائمة أو تقلل قيمة النظام وتفسخ خدماته وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات.

¹¹ - علاء حسين الحمادي وآخرين، تكنولوجيا أمنية المعلومات أنظمة الحماية ،دار وائل عمان، 2007 ،ص 42-45

الفرع الأول: ماهية المخاطر نظم المعلومات :

تتجه العديد من الشركات إلى الاعتماد على تكنولوجيا المعلومات من خلال نظم معلومات متكاملة ، والتي تؤدي إلى دقة وسرعة تشغيل العمليات ، وبالتالي تحقيق العديد من المزايا التنافسية للشركات ، ومع ذلك فإنه تطبيق تكنولوجيا المعلومات يصاحبه العديد من المخاطر.

تعرف المخاطر بصفة عامة بأنها احتمال وقوع حدث ما أو تصرف ما من شأنه أن يؤدي إلى فشل المنظمة في تحقيق أهدافها وهناك العديد من المخاطر التي تواجه الشركات ، تتمثل في الآتي:¹²

- ✓ المخاطر الإستراتيجية Strategic risk
- ✓ المخاطر البيئية Environmental risk
- ✓ المخاطر السوق Market risk
- ✓ مخاطر التشغيل Operational risk
- ✓ مخاطر الائتمان Credit risk
- ✓ مخاطر الالتزام Compliance risk

وتعد مخاطر تكنولوجيا المعلومات أحد أنواع المخاطر التي تواجه الشركات ، والتي قد تكون جزءاً من أحد المخاطر السابقة.

وتعرف مخاطر تكنولوجيا المعلومات بصفة خاصة على أنها " كل ما ينتج عنه وجود خطأ أو خلل في تكنولوجيا المعلومات تؤدي إلى تأثير سلبي على أعمال المنظمة ، ولقد جاء تعريف جمعية مراجعة ومراقبة نظم المعلومات ISACA لمخاطر نظم المعلومات متسقاً مع ما سبق ، وعرفت على أنها:

" احتمال حدوث تصرف ما أو حدث ما له تأثير سلبي على المنظمة وعلى نظم المعلومات الخاصة بها ، أي احتمال أن يحدث استغلال لنقاط الضعف في الأصل أو مجموعة من الأصول فيسبب خسائر أو أضرار للأصول "

ويتطلب الكشف عن الأبعاد المختلفة لمخاطر نظم المعلومات تناول المقومات الأساسية لأي نظام معلومات وهي :¹³

1- الأفراد : وهم الذين يقومون بتشغيل النظام ، وأداء الوظائف المختلفة.

2- الإجراءات : تتضمن تلك الإجراءات سواء في النظام اليدوي أو النظام الآلي تجميع وتشغيل وتخزين البيانات عن أنشطة المنظمة .

¹² -علا محمد شوقي ابراهيم عيسى ، تأثير تطبيق حوكمة الشركات على مخاطر نظم المعلومات المحاسبية ، دار الجزائرية للنشر والطبع والتوزيع، الجزائر، 2015، ص 63

¹³ مصطفى فتحي ، أمن المعلومات ، دورة علمية ، المنظمة العربية للتنمية الإدارية، القاهرة ، 2010 ص 10

3-البيانات : وهي تتعلق بالعمليات التي تقوم بها المنظمة.

4-البرامج : وهي التي تستخدم في تشغيل بيانات النظام.

5-البنية التحتية لتكنولوجيا المعلومات : وهي تشمل أجهزة الكمبيوتر ، وملحقاتها ، ووسائل اتصالات الشبكات.

وتتسم أسباب مخاطر تكنولوجيا المعلومات والآثار الناتجة عنها بالتعقيد ، وبصفة خاصة في المنظمات كبيرة الحجم ، ويمكن تقسيم أسباب مخاطر تكنولوجيا المعلومات إلى أسباب خارجية تنبع من البيئة الخارجية ، وأسباب داخلية مصدرها البيئة الداخلية

الفرع الثاني: المخاطر نظم المعلومات:

أولاً: من حيث مصدرها: توجد عدت المخاطر نظم المعلومات تختلف من حيث المصدر:¹⁴

1: **مخاطر داخلية:** حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات الحاسوبية الإلكترونية وذلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنشأة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها .

2: **مخاطر خارجية :** وتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قرصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة أو قد تتمثل في كوارث طبيعية مثل الزلازل والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشأة.

ثانياً: من حيث المتسبب لها

1. **مخاطر ناتجة عن العنصر البشري:** وتلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ.

2. **مخاطر ناتجة عن العنصر غير البشري:** وهي تلك المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه

ثالثاً: من حيث العمدية (القصد)

1. **مخاطر ناتجة عن تصرفات متعمدة(مقصودة):** و تتمثل في تصرفات يقوم بها الشخص متعمداً مثل إدخال بيانات خاطئة وهو يعلم ذلك، أو قيامه بتدمير بعض البيانات متعمداً ذلك بهدف الغش والتلاعب والسرقة، وتعتبر هذه المخاطر من المخاطر المؤثرة جداً على النظام

¹⁴ - حرية شعبان محمد الشريف ، مرجع سبق ذكره، ص 84

2. مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة): وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق ادخالها أو السهو في عملية التسجيل وتعتبر هذه المخاطر أقل ضررا من المخاطر المقصودة وذلك لإمكانية إصلاحها.

رابعا: من حيث الآثار الناتجة عنها: تتعدد وتنفرد المخاطر من حيث الآثار الناتجة عنها¹⁵:

1. مخاطر تنتج عنها أضرار مادية: وهي المخاطر التي تؤدي إلى حدوث أضرار للنظام وأجهزة الكمبيوتر أو تدمير لوسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للإنسان بها أو قد تكون بسبب البشر بطريقة متعمدة أو عفوية:

2. مخاطر فنية ومنطقية: وهي المخاطر الناتجة عن أحداث قد تؤثر على البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها وذلك من خلال تعطيل في ذاكرة الكمبيوتر أو إدخال فيروسات للكمبيوتر قد تفسد البيانات أو جزء منها وتلك المخاطر قد تؤثر على الموقف التنافسي للمنشأة وقد تحدث المخاطر السابقة من خلال قيام المهاجم بالبحث في مخلفات التقنية الخاصة بالمؤسسة من قمامة وأوراق متروكة بهدف الحصول على أية معلومات قد تساعد على اختراق النظام للحصول على كلمات السر المدونة على الأوراق الملقاة أو الأقراص الصلبة التي يتم استبدالها، أو أي معلومة أخرى تساهم في اختراق النظام والتي تعرف بتقنية القمامة، ونستطيع أن ندرك درجة خطورة تقنية القمامة من خلال معرفة ما حصل مع وزارة العدل الأمريكية.

حيث قامت وزارة العدل الأمريكية ببيع مخلفات أجهزة تقنية بعد أن تقرر إتلافها وكان من ضمن تلك المخلفات جهاز كمبيوتر يحتوي قرصه الصلب على كافة العناوين الخاصة ببرامج حماية الشهود وخوفا من نشر تلك المعلومات أو استثمارها ضد الوزارة فقد قامت وزارة العدل بنقل كافة الشهود وتغيير مكان أقامتهم وهوياتهم وهذا تطلب تكلفة مالية ضخمة وذلك بسبب الإخفاق في إتلاف الأقراص بطريقة صحيحة.

خامسا: المخاطر من حيث علاقتها بمراحل النظام : لمخاطر علاقة من حيث مراحل نظم المعلومات نذكر منها¹⁶

1. مخاطر المدخلات: وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال وتتمثل المخاطر المتعلقة بأمن المدخلات إلى أربعة أقسام أساسية وهي:

¹⁵ - رجم خالد، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2017 ص71

¹⁶ - عصام محمد البيحيصي و أ. حرية شعبان الشريف "مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة" مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية) المجلد السادس عشر، العدد الثاني، . 2008 الجامعة الإسلامية - غزة - فلسطين.ص904-905

أ- خلق بيانات غير سليمة:

ويتم ذلك من خلال خلق بيانات غير حقيقية ولكن بواسطة مستندات صحيحة يتم وضعها داخل مجموعة من العمليات دون أن يتم اكتشافها، ومثال ذلك استخدام أسماء وهمية لموظفين لا يعملون بالشركة وإدراج تلك الأسماء ضمن كشف الرواتب وصرف رواتب شهرية لهم أو إدخال فواتير وهمية باسم أحد الموردين.

ب- تعديل أو تحريف البيانات المدخلات:

ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسؤول وقبل إدخالها إلى النظام، وذلك عن طريق تغيير في أرقام مبالغ بعض العمليات لصالح المحرف، أو تغيير أسماء بعض العملاء أو معدلات الفائدة.

ت- حذف بعض المدخلات :

ويحدث ذلك من خلال حذف أو استبعاد بعض البيانات قبل إدخالها إلى الحاسب الآلي، وذلك إما بشكل متعمد ومقصود أو بشكل غير متعمد وغير مقصود، ومثال ذلك قيام الموظف المسؤول عن المرتبات في المنشأة بتدمير مذكرات وتعديلات تفصيلات حساب البنك لحساب آخر خاص بالموظف المحرف.

ج- إدخال البيانات أكثر من مرة:

والمقصود بذلك قيام الموظف بتكرار إدخال البيانات إلى الحاسب إما بطريقة مقصودة أو غير مقصودة، ويتم ذلك من خلال إدخال بيانات بعض المستندات أكثر من مرة إلى النظام قبل أوامر الدفع وذلك إما بعمل نسخ إضافية من المستندات الأصلية وتقديم كل من الصورة والأصل أو إعادة إدخال البيانات مرة أخرى إلى النظام.

2. مخاطر تشغيل البيانات: ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتمثل مخاطر تشغيل البيانات في الاستخدام غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي، ومثال على ذلك قيام الموظف بإعطاء أوامر للبرنامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميل معين من أجل الاستفادة من مبلغ العملية لصالح المحرف نفسه.

3. مخاطر مخرجات الحاسب: ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استخدامها أو عمل نسخ غير مصرح بها من المخرجات أو الكشف الغير مسموح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق أو طبع وتوزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك، كذلك توجيه تلك المطبوعات والمعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات أو تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمريرها أو التخلص منها مما يؤدي إلى استخدام تلك المعلومات في أمور تسيء إلى المؤسسة وتضر بمصالحها.

سادسا: مخاطر نظم المعلومات حسب الغرض منها

تعرض نظم المعلومات الحاسوبية إلى العديد من الأخطار وتهديدات التي قد تهدد أمن نظم معلوماتها، وقد تتنوع مصادر تلك تهديدات بحسب الأغراض التي تقوم بها تلك النظم ويمكن تصنيف أنواع التهديدات والأخطار بحسب مصادرها إلى أربعة أنواع رئيسية:¹⁷

- ✓ حرق النظم الحاسوبية بهدف الاطلاع على المعلومات المخزنة فيها والوصول إلى معلومات شخصية أو أمنية عن شخص ما، أو التجسس الصناعي، أو التجسس المعادي للوصول إلى معلومات عسكرية سرية.
- ✓ حرق النظم الحاسوبية بهدف التزوير أو الاحتيال) التلاعب بالحسابات في البنوك، التلاعب بفاتورة الهاتف، التلاعب بالضرائب، تغيير بيانات شخصية من السجل المدني أو السجل العام للموظفين، إلخ
- ✓ حرق النظم الحاسوبية بهدف تعطيل هذه النظم عن العمل لأغراض تخريبية باستخدام ما يسمى البرامج الخبيثة) مثل الفيروسات، الدودة، حصان طروادة، أو القنابل الإلكترونية (إما من قبل الأفراد أو العصابات أو الجهات الأجنبية بغرض شل هذه النظم الحاسوبية) أو المواقع على الانترنت (عن العمل وخاصة في ظروف خاصة أو في أوقات الحرب.
- ✓ أخطار ناتجة عن فشل التجهيزات في العمل، أعطال كهربائية، حريق، كوارث طبيعية) فيضانات، زلزال

ومن خلال ماسبق تصنيف المخاطر التي تواجه نظم المعلومات الإلكترونية بشكل عام إلى أربعة أصناف رئيسية:

1-6: مخاطر المدخلات: وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة إدخال البيانات إلى النظام

الآلي وتمثل تلك المخاطر في البنود التالية:

- ✓ الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
- ✓ الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
- ✓ التدمير غير المتعمد للبيانات بواسطة الموظفين.
- ✓ التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين

2-6 مخاطر تشغيل البيانات: وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة

البيانات المخزنة في ذاكرة الحاسب وتمثل تلك المخاطر في البنود التالية¹⁸:

- ✓ المرور الوصول (غير الشرعي) (غير المرخص به) للبيانات والنظام بواسطة الموظفين.
- ✓ المرور غير الشرعي (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج المنشأة.
- ✓ اشتراك العديد من الموظفين في نفس كلمة السر.

¹⁷ - يزيد دكار ،تقييم كفاءة نظام المعلومات الإلكتروني ،مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير،ورقلة، 2016 ص12

¹⁸ - رجم خالد ، محاضرات أمن المعلومات ، محاضرات مقياس مراجعة نظام المعلومات سنة أولى ماستر تدقيق ومراقبة التسيير، جامعة ورقلة 2015، -2016

- ✓ إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام.
- ✓ اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

3-6 مخاطر مخرجات الحاسب: وتلك المخاطر تتعلق بمرحلة مخرجات عمليات معالجة وتشغيل البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات مغمطة وكيفية استلام تلك المخرجات وتتمثل تلك المخاطر في البنود التالية:

- ✓ طمس أو تدمير بنود معينة من المخرجات.
- ✓ خلق مخرجات زائفة /غير صحيحة.
- ✓ سرقة البيانات /المعلومات.
- ✓ عمل نسخ غير مصرح (مصرح) بها من المخرجات.
- ✓ الكشف غير المصرح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.
- ✓ طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.
- ✓ المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم/ ليس لهم الحق في استلام نسخة منها.
- ✓ تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها

4-6: مخاطر بيئية: وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل الزلازل والعواصف والفيضانات والأعاصير المتعلقة بأعطال التيار الكهربائي والحرائق، وسواء كانت تلك الكوارث طبيعية أو غير طبيعية فإنها قد تؤثر على عمل النظام وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات الالكترونية.

الفرع الثالث: أسباب حدوث المخاطر نظم المعلومات

تعرض نظم المعلومات للعديد من المخاطر التي تهدد أمنها وقد قمنا بتقسيم تلك المخاطر إلى أربعة أقسام رئيسية تتعلق بمراحل النظام الأساسية من إدخال وتشغيل ومخرجات والقسم الرابع يتعلق بالمخاطر البيئية وقد ترجع أسباب حدوث تلك المخاطر إلى أسباب تتعلق بالمدخلات والمخرجات وأسباب تتعلق بالتشغيل أو قد نعتبرها أسباب إدارية رقابية وأسباب لها علاقة بالموظفين،

وتتلخص تلك الأسباب في البنود التالية: ¹⁹

- ✓ عدم كفاية وفعالية الأدوات الرقابية المطبقة لدى إدارة المنشأة.
- ✓ ضعف نظم الرقابة الداخلية لدى المنشأة وعدم فعاليتها.
- ✓ اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظام والعبث بمحتوياته.
- ✓ عدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات في المنشأة.
- ✓ عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيما يختص بأمن نظم المعلومات الحاسوبية لدى المنشأة.
- ✓ عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر.
- ✓ ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب.
- ✓ عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات.
- ✓ عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة.
- ✓ عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي المنشأة
- ✓ عدم إلزام الموظفين بأخذ إجازاتهم الدورية.
- ✓ عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.
- ✓ عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي المنشأة.
- ✓ عدم وجود الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.

الفرع الرابع: تهديدات نظم المعلومات

تتعدد الوسائل وأساليب القرصنة في الاختراق أمن المعلومات كما هو موضح في الشكل ص 21 رقم (1-6)، إلا أنها في مجملها تهدف إلى مهاجمة هذه الأهداف وتحقيق نفع معين للمهاجم من وراء ذلك، وفي بعض الأحيان لا يكون الهدف من الاختراق نفع معين للمهاجم سوى تعريض المستهدف للخطر والضرر، تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة ومن أهم الأساليب والطرق ما يلي:

¹⁹ - حرية شعبان محمد الشريف، مخاطر نظم المعلومات المحاسبية الإلكترونية "دراسة تطبيقية على المصارف العاملة في قطاع غزة"، مذكرة ماجستير منشورة، كلية التجارة بالجامعة الإسلامية بغزة، 2006، ص 84

أولاً : البرامج الخبيثة :

وهي عبارة عن برامج تم إعدادها من قبل مبرمجين وذلك لغرض إلحاق الضرر بالبيانات المستهدفة كتخريبها وإزالتها أو السيطرة عليها وإلحاق الضرر بها . وتتميز هذه البرامج بقدرتها على التناسخ والانتشار والانتقال من مكان إلى آخر . ويمكن تقسيم هذه البرامج إلى عدة أنواع وذلك بحسب سلوكها ومنها انظر الجدول رقم (1-2) في ص22:²⁰

ثانياً: أنواع الهجوم Attacks

توجد مجموعة من الهجمات التي يستعملها المتجسسون على المستهدفون من أجل إلحاق الضرر وتجسس على نظام المعلومات ونذكر منها²¹ :

1- هجوم التصنت على الرسائل: Attacks Interception

وفكرة عمل هذا الهجوم: أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال Eavesdropping

2- هجوم توقيف: Interruption Attacks

وهذا النوع يعتمد على قطع قناة الاتصال إيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة²²

3- هجوم يعدل على محتوى الرسالة: Modification Attacks

فإنه هنا يتدخل المهاجم بين المرسل والمستقبل يعتبر وسيط بين المرسل والمستقبل وعندما تصل إلى Attacker يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل ، والمستقبل طبعاً يعلم بتعديل الرسالة من قبل Attacker.

4- الهجوم المزور أو المفبرك: Fabrication Attacks

وهنا يرسل المهاجم رسالة مفادها انه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة²³ .

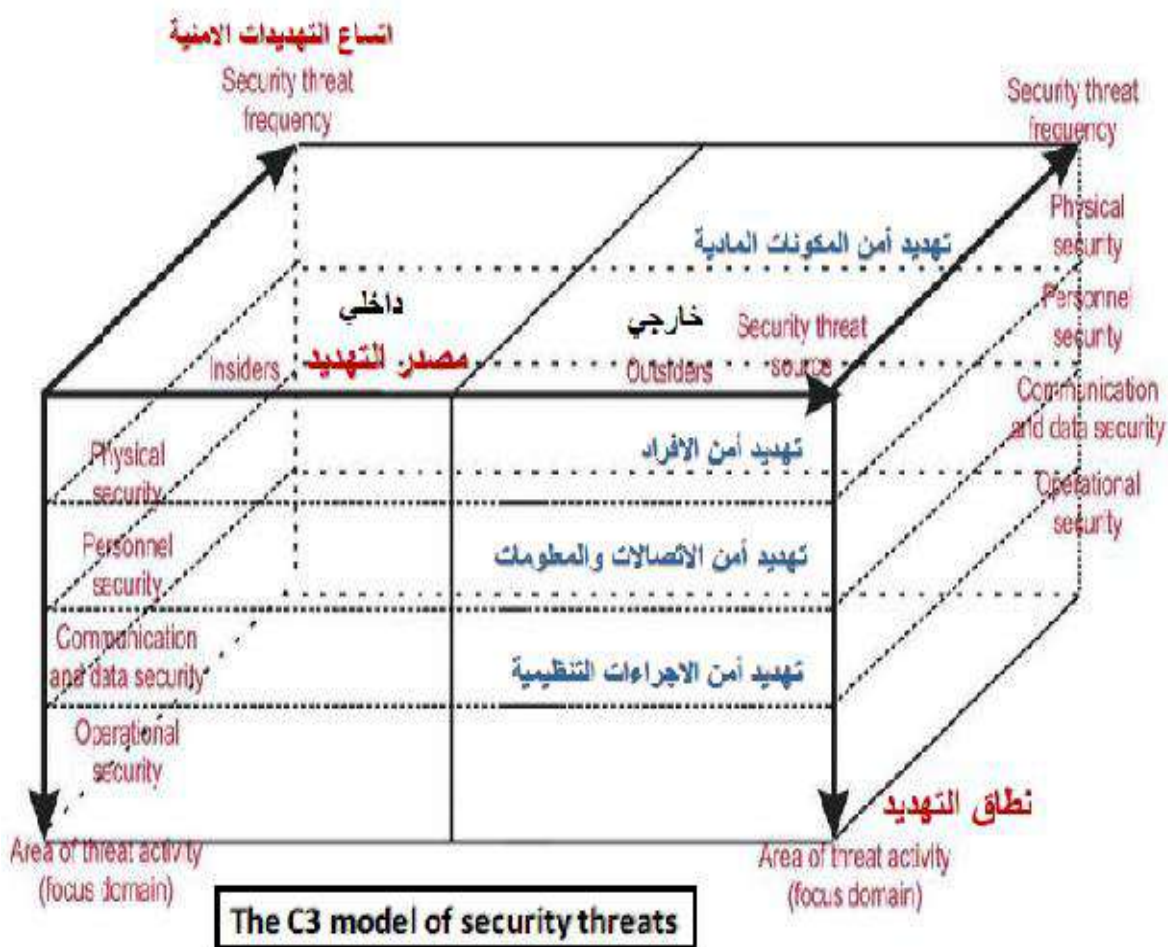
20- مصطفى فتحي ، أمن المعلومات ، دورة علمية ، المنظمة العربية للتنمية الإدارية، القاهرة ، 2010 ص13

21- مصطفى فتحي ، نفس المرجع

22- رجم خالد ، محاضرات أمن المعلومات ، محاضرات مقياس مراجعة نظام المعلومات سنة أولى ماستر تدقيق ومراقبة التسيير ، جامعة ورقلة 2015 ، -2016

23- رجم خالد ، نفس المرجع

الشكل رقم (5-1): يوضح النموذج ثلاثي الأبعاد لتصنيف تهديدات نظم المعلومات



المصدر: أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية، أطروحة ماجستير، كلية التجارة
، غزة، 2013 ص 60

الفصل الأول: الأدبيات النظرية و التطبيقية لمساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظام المعلومات

الجدول رقم 1-2: أنواع البرامج الخبيثة

البرامج الخبيثة	تعريف	مصادرها	تأثيرها على الأمن المعلومات
01 - الفيروسات	هو برنامج صغير مكتوب بأحد اللغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب وهو مصمم على إن يقوم بأعدته كتابة نفسه على الملفات الموجودة على الحاسب أو أى حاسب آخر يتم تبادل المعلومات بينه وبين الحاسب حامل الفيروس.	- من خلال الرسائل الإلكترونية - صفحات الانترنت "HTTP" - نسخ البرامج المقلدة - الأقراص المرنة والأقراص الضوئية	- زيادة عدد العمليات التي تتم إلى ملايين العمليات فيتوقف الحاسب عن العمل - إلغاء بعض ملفات النظام - زيادة حجم الملف بإعادة كتابته على نفسه آلاف المرات - إغلاق الحاسب من تلقاء نفسه عند الدخول على الانترنت مثلا - إلغاء البرنامج المكتوب على BIOS
02- ديدان الانترنت	هي مثلها مثل الفيروس برنامج صغير مكتوب بأحد اللغات الحاسب مصمم على إن يقوم بالاعادة كتابة نفسه على الملفات الموجودة على الحاسب أو أى حاسب آخر ولكنها متميزة بكونها ترسل نفسها منفردة إلى قائمة البريد الإلكتروني أو إلى كل جهاز بالشبكة وهي تنتشر بسرعة هائلة	- من خلال الرسائل الإلكترونية - صفحات الانترنت "HTTP" - نسخ البرامج المقلدة - الأقراص المرنة والأقراص الضوئية	- زيادة عدد العمليات التي تتم إلى ملايين العمليات فيتوقف الحاسب - التحميل الزائد على الشبكة مما قد يبطئ العمل عليها تماما - إحداث البطء الشديد في الانترنت داخل المؤسسة أو على الحاسب الشخصي
03-أحصنة طروادة	هو برنامج حاسوب موضوع في احد البرامج التي تستخدم مثل الألعاب ولكن بداخلها تكسر الحماية المستخدمة لديك كما تدمر الملفات	- وهي تأتي غالبا مع الرسائل الإلكترونية المرفق معها ملفات قابلة للتشغيل لذا لا تفتح أى ملف مرفق مع الرسائل الإلكترونية إذا كانت ملفات قابلة للتشغيل. - وهي تأتي أيضا عند تحميلك للبرامج المجانية الموجودة على الانترنت لذا لا تحمل أى برنامج مجاني من الانترنت إذا كنت لا تعرف وتثق في الموقع الموجود عليه هذا البرنامج	- يقوم بإلغاء الملفات - يرسل رسائل مزيفة منك إلى الموجودين في قائمة البريد الإلكتروني - يفتح الحماية الخاصة بك لمخترقي الحاسوب
05- البريد الإلكتروني غير المرغوبة Spam E-mail	استقبال مجموعة من الرسائل الإلكترونية "إعلانات" من عناوين وهمية متجددة في كل مرة	- انتشار العنوان البريدي على الانترنت في احد المواقع التي تم اختراقها واخذ كافة العناوين ووضعها قائمة الإرسال أو تباع من ISP أو احد الشركات المسجل بها بيانات المستخدم.	- استقبال رسائل غير مرغوب بها . - شغل حيز من مصدر الانترنت المستخدم بالمؤسسة
06- الباب الخلفي Backdoor	وهي عبارة عن الثغرات الموجودة بقصد أو غير قصد في أنظمة التشغيل , ويعد هذا النوع هو الأخطر والأكثر شيوعا لدى المخترقين حيث تمكنهم من القدرة على الدخول والسيطرة على الأجهزة كليا أو جزئيا وذلك بحسب البرنامج المستخدم.	- نسخ البرامج المقلدة - من خلال الرسائل الإلكترونية - الأقراص المرنة والأقراص الضوئية	- يرسل رسائل مزيفة منك إلى الموجودين في قائمة البريد الإلكتروني - يفتح الحماية الخاصة بك لمخترقي الحاسوب - إحداث البطء الشديد في الانترنت داخل المنشأة أو على الحاسب الشخصي

المصدر : من إعداد الباحث بالاعتماد على مصطفى فتحي ، أمن المعلومات ، دورة علمية ، المنظمة العربية للتنمية الإدارية، القاهرة ، 2010

المبحث الثاني: الدراسات السابقة:

المطلب الأول: الدراسات السابقة باللغة العربية :

الفرع الأول:

دراسة (أيمن محمد فارس الدنف 2013) بعنوان "واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها" وهدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، وأستخدم الباحث المنهج البحثي الوصفي التحليلي، وتكون مجتمع الدراسة من العاملين على نظم المعلومات في الكليات التقنية وجمعت أدوات الدراسة بين الاستبانة والمقابلة ، وتوصلت الدراسة إلى مجموعة من النتائج أهمها، أن تتوفر البنية التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة، وأن 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 بمجتمع الدراسة في درجات استخدام تعهد نظم معلوماتها، وإن توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة.

الفرع الثاني:

دراسة (حرية شعبان محمد الشريف 2006) بعنوان "مخاطر نظم المعلومات المحاسبية الإلكترونية دراسة تطبيقية على المصارف العاملة في قطاع غزة" تهدف هذه الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر حيث استعانت الباحثة بما تناولته الدراسات السابقة والأبحاث التي اهتمت في هذا المجال، كذلك تم التعرف على الإجراءات والوسائل الرقابية المتبعة من قبل المصارف العاملة في قطاع غزة لمواجهة تلك المخاطر التي قد تواجه نظم معلوماتها المحاسبية الإلكترونية وبناء على ذلك تم استخلاص بعض النتائج التي تسهم في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة، وتقديم التوصيات في هذا المجال كما استخدمت الدراسة المنهج الوصفي التحليلي في الوصول لنتائج الدراسة، حيث تم توزيع استبانة على المصارف العاملة في قطاع غزة وفروعها وقد تم استخدام برنامج التحليل الإحصائي (SPSS) للعلوم الإنسانية والاجتماعية لمعالجة البيانات باستخدام التكرارات والنسب المئوية، والمتوسطات الحسابية، واختبار الإشارة إلى معلمي (Sign Test) وقد تم التوصل إلى مجموعة من النتائج أهمها، أوضحت الدراسة قلة عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة حيث يعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفين المختصين يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية ، وأن الإدارة الجيدة تستطيع أن تقلل أو تحدد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف ، وأن تطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية.

الفرع الثالث :

دراسة (هاني عبد الرحمن محمد أبو عمر 2009) بعنوان "فاعلية نظم المعلومات الإدارية المحوسبة وأثره في إدارة الأزمات دراسة تطبيقية على القطاع المصرفي في فلسطين" هدفت هذه الدراسة إلى قياس مدى فاعلية نظم المعلومات الإدارية المحوسبة وأثرها في قدرة المصارف العاملة في فلسطين على إدارة أزماتها. وتم تصميم مقياس مكون من ستة عناصر وهي : (سرعة الحصول على المعلومات، سرعة اتخاذ القرارات، رضا المستخدم، مدى ملائمة النظام للمستويات الإدارية، الاستجابة للتغيرات المستجدة، أمن المعلومات لقياس فاعلية نظم المعلومات الإدارية المحوسبة ،) حيث تم استخدام المنهج الوصفي التحليلي، وطبقت الدراسة على جميع المصارف العاملة في فلسطين والبالغ عددها 21 مصرفاً، وقد بلغ مجتمع الدراسة 348 موظفاً، حيث تم أخذ عينة طبقية عشوائية مكونة من 186 موظف بواقع 53% من مجتمع الدراسة الكلي.

وتم تصميم استبانته لهذا الغرض وكان من أهم نتائج الدراسة، وجود علاقة قوية ذات دلالة إحصائية بين فاعلية نظم المعلومات الإدارية وبين قدرة المصارف العاملة في فلسطين على إدارة الأزمات وخلصت الدراسة إلى أن ما نسبته % 66.6 من قدرة المصارف على إدارة الأزمات يفسره فاعلية نظم المعلومات الإدارية المحوسبة والباقي يعود لعوامل أخرى.

الفرع الرابع :

دراسة (مقراني قدور 2015) بعنوان "تقييم مدى مساهمة أمن نظم المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات دراسة حالة مؤسسة اتصالات الجزائر" هدفت هذه الدراسة إلى تقييم أمن نظام المعلومات في مؤسسة اتصالات الجزائر، حيث إلى تطرقت إلى المخاطر المحدقة بنظام المعلومات والإجراءات التي من شأنها الحد من هذه المخاطر، ومن محاولة إسقاط هذه المعطيات على نظام المعلومات داخل المؤسسة المعنية بالدراسة، وقد اعتمد الباحث على المنهج الوصفي في الجانب النظري من أجل تسليط الضوء على نظم المعلومات ومخاطرها والعناصر الأمنية، وأثناء إعداد هذه الدراسة تم توزيع الاستبيان الذي تمثل في 100 استمارة أهم النتائج المتوصل إليها هي أن السياسات الأمنية داخل نظام المعلومات من شأنها ضمان ديمومة عمل هذا النظام في ظروف مثلى مع إشراك العامل البشري في هذه السياسات.

المطلب الثاني : الدراسات السابقة باللغة الأجنبية

الفرع الأول:

دراسة (Kreicberga 2010) بعنوان " التهديدات الداخلية لأمن المعلومات-التدابير المضادة والعنصر البشري" تحدد الغرض العام من الدراسة لاستيضاح المعرفة حول دور العامل البشري في حقل أمن نظم المعلومات وتساءلت الدراسة حول العوامل التي تؤثر على السلوك الأمني للموظفين ؟ ، وكيف ينظروا تجاه التدابير الأمنية المضادة للتهديدات الداخلية ؟ واستخدم المنهج الكيفي (النوعي) وكانت أداة المقابلة التي أجريت مع مسؤولي أمن المعلومات والمستخدمين بالإضافة لمراجعة وتحليل الوثائق والمستندات ، والملاحظة المباشرة لسلوك المستخدمين وتوصلت الدراسة إلى ، رضا وقبول الموظفين والتدابير الأمنية عناصر

مهمة في تحقيق سلوك أمن تجاه أمن نظم المعلومات، وأن يواجه الموظفون صعوبة ومقدار من التعقيد في فهم الوثائق المتعلقة بأمن المعلومات، تطبيق المتطلبات البشرية لأمن المعلومات يحتاج إلى حالة وعي بأهمية أمن نظم المعلومات.

الفرع الثاني:

دراسة (Lan 2007) بعنوان: "إدارة أمن نظم المعلومات في الجامعات الاسترالية" هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الجامعات الأسترالية، وما هي العوامل الأساسية التي تؤثر في فعاليتها، وكيف يمكن تحسينها، وأجريت الدراسة على 38 جامعة أسترالية، وطرحت الأسئلة على رئاسات الجامعات ومديري أقسام تكنولوجيا المعلومات ومسؤولي أمن المعلومات، عبر مقابلة استخدم فيها أسلوب الأسئلة المفتوحة والمغلقة، وتوصلت الدراسة للنتائج التالية: يختلف واقع إدارة أمن المعلومات من جامعة لأخرى ويعود ذلك لعدة عوامل منها ، منهجية الإدارة الأمنية، واهتمام الإدارة العليا وانخراطها، وحجم الإنفاق على أمن المعلومات، والجهد المبذول على مواجهة التهديدات الأمنية، ومستوى أهمية تكنولوجيا المعلومات، والثقافة العامة للمؤسسة ، أهم العوامل المؤثرة في فاعلية دور إدارة أمن المعلومات تعود لأسباب :

نقص الخبرات وضعف هيكلية إدارة أمن المعلومات، و وجود فجوة بين ما هو مأمول وما هو معمول به من وعي بأمن المعلومات وسبب ذلك هو قلة الاكتراث بالمخاطر والتهديدات، وتطوير السياسات الأمنية بشكل واضح وقابل للعمل ويتم الامتثال له ضمن القواعد الأمنية والقانونية، وأن للتغلب على ضعف إدارة أمن نظم المعلومات فإنه من الضروري تطوير فاعلية العناصر والكوادر البشرية كأحد أهم مرتكزات إدارة أمن نظم المعلومات.

الفرع الثالث:

دراسة (Mwita Simion Maroa 2015) بعنوان "العوامل المؤثرة في فاعلية أمن نظم المعلومات في جامعة نيروبي" عاجلت هذه الدراسة العوامل المؤثرة في أمن المعلومات أخذت كدراسة حالة جامعة نيروبي ، بمحاولة قياس أثر السياسات الأمنية على الفعالية الأمنية المتبعة في الجامعة نيروبي ، وقد تمثل مجتمع الدراسة المستهدف جميع مستعملي نظام المعلومات في جميع الكليات والإدارات الملحقه بجامعة نيروبي لسنة 2015، واستعملت الدراسة المنهج الوصفي ، كما استعمل الباحث أسلوب الاستبيان حيث تم توزيع استبيان 130، وتمكن استرجاع 120 وقد توصل الباحث إلى أهم النتائج وتمثلت في أن دعم الإدارة العليا والسياسات الأمنية لنظم المعلومات وتدريب المستخدمين وزيادة الوعي يؤثرون على فاعلية أمن نظم المعلومات في الجامعة نيروبي لكن بدرجات مختلفة ، حيث يزداد تأثير العوامل الثلاثة الأخيرة بقوة مقارنة بعامل دعم الإدارة العليا

المطلب الثالث: مقارنة الدراسة الحالية بالدراسات السابقة :

من خلال هذا المطلب سنحاول إبراز أهم أوجه التشابه والاختلاف بين الدراسات السابقة وهذه الدراسة وتكون على النحو

التالي:

الفرع الأول: أوجه التشابه :

تمثلت أوجه التشابه بين دراستنا و الدراسات السابقة كما يلي:

- يتضح من الدراسات السابقة والدراسة الحالية التي تم عرضها أن هناك اهتمام متزايد وتوجه ايجابي الدراسة أمن المعلومات، وهذا الاهتمام لا يقتصر على نوع بعينه من المؤسسات بل يشمل المؤسسات الحكومية، وغير الحكومية، والربحية وغير الربحية والمؤسسات التعليمية والصحية والخدمية
- أظهرت الدراسات السابقة والحالية أهمية موضوع أمن المعلومات كونه يمس عضد المؤسسات في عصر الرقميات وأعتبرت نظم المعلومات إحدى مقومات بقاؤها
- كل الدراسات السابقة والحالية تم اعتمادها في الجانب النظري على عموميات التي لها علاقة مباشرة بأمن المعلومات الإلكتروني ومخاطر نظم المعلومات
- تم اعتماد في الجانب التطبيقي في الدراسات السابقة والحالية على الاستبيان في جمع المعلومات
- ركزت الدراسات السابقة والحالية على معوقات ومهددات تحقيق أمن المعلومات من جهة، ومن جهة أخرى بينت مدى فعالية إدارة أمن المعلومات قياساً لتطبيق معايير دولية بهذا الشأن، أو ستطرق البعض متخصصاً الدراسة أثر العنصر البشري في تحقيق كفاءة نظم أمن المعلومات

الفرع الثاني: أوجه الاختلاف :

تمثلت أوجه الاختلاف بين دراستنا و الدراسات السابقة كما يلي:

- ✓ تم الاعتماد في دراسة الحالة في جميع الدراسات السابقة على مؤسسة واحدة ولكن في الدراسة الحالية دراسة مقارنة بين أكثر من مؤسستين كبيرتين
- ✓ تم الاعتماد في الدراسة الاستبيان والمقابلة والملاحظة في جمع المعلومات في عينة الدراسة
- ✓ إبراز أهمية الأمن المعلومات في المؤسسات محل الدراسة
- ✓ التعرف على الإجراءات وخطوات الأمن المعلومات في المؤسسات

خلاصة الفصل:

تطرقنا خلال هذا الفصل لمختلف المفاهيم المتعلقة بنظام المعلومات ومكوناته، وكذلك المخاطر التي تتهدد النظام عبر عدة تصنيفات كان أهمها المخاطر وتهديدات متعلقة بمراحل النظام من مدخلات ومعالجة ومخرجات، ثم التهديدات التي يمكن أن يتعرض لها النظام وقد تناولنا فيها الوصول غير الشرعي، والبرمجيات الخبيثة كالفيروسات وأحصنة طروادة، وفي باب آخر تم التطرق لمفهوم أمن المعلومات، وعناصره ومكوناته، وكيفية تصميم نظام الحماية، وفي الأدبيات التطبيقية تناولنا في المجلد سبع دراسات سابقة منها أربعة باللغة العربية وثلاثة باللغة الأجنبية رسمة في مجملها نظرة على موضوع أمن نظم المعلومات من زوايا مختلفة.

وبعد استعراضنا للجانب النظري للموضوع في الفصل الأول، سنحاول في الفصل التالي الوقوف على الدراسة الميدانية التي عاجلت تقييم أمن نظام المعلومات في الحد من المخاطر في مؤسسات محل الدراسة .



الفصل الثاني: الدراسة الميدانية لتقييم اثر

الأمن الالكتروني في الحد من المخاطر النظم

المعلومات

تمهيد :

في الفصل الأول تطرقنا للإطار النظري لنظام المعلومات ومكوناته والأمن الإلكتروني ، كما تناولنا المفاهيم الأساسية لنظام المعلومات الإلكتروني وعناصره، بالإضافة إلى التعريف بمكوناته وعرض أهم الإجراءات المتعلقة بأمن وسلامة نظام المعلومات الإلكتروني وفي نهاية الفصل استعرضنا بعض الدراسات السابقة التي لها علاقة وصلة بموضوع الدراسة.

أما في هذا الفصل سنحاول إسقاط الدراسة النظرية على أرض الواقع، وقد وقع اختيارنا على مجموعة من مؤسسات ناشطة في التراب ولاية ورقلة ، محاولين التعرف على نظامها المعلوماتي الإلكتروني، والسياسات الأمنية المتبعة ، ومن أجل الوصول إلى ذلك سنتطرق في المبحث الأول لطريقة الدراسة والأدوات المستعملة فيها، و نستعرض أهم النتائج التي توصلنا لها من خلال استعمال أداة المقابلة في تشخيص نظام المعلومات والسياسات الأمنية لمؤسسات محل الدراسة ، وفي المبحث الثاني نقوم بعرض نتائج أداة الاستبيان لمعرفة مدى مساهمة الأمن الإلكتروني في الحد من المخاطر نظم المعلومات في المؤسسات محل الدراسة .

المبحث الأول : الطريقة والأدوات المستخدمة في الدراسة :

نتطرق في هذا المبحث للطريقة و الأدوات المستخدمة في هذه الدراسة، حيث يتضمن التعريف بمجتمع وعينة الدراسة، كما يوضح الأدوات الإحصائية والبرامج المستخدمة في الدراسة.

المطلب الأول : عينة الدراسة :

أما عن عينة الدراسة الميدانية التي شملها الدراسة، فتتمثل في مجموعة من شركات محل الدراسة التي شملت كل من اتصالات الجزائر- ورقلة/ الشركة الوطنية للكهرباء والغاز - ورقلة / ليند غاز- وحدة ورقلة والتي كانت عينة قصدية تخص عينة من مستخدمي نظام المعلومات الإلكتروني لمؤسسة والمسؤولين على نظام المعلومات تم توزيع استمارات الاستبيان بحجم عدد العينة ويمثل العدد الإجمالي للمسؤولين على نظام المعلومات ومستخدمي نظام في شركات سالفه ذكر التي اختيرت كعينة دراسة سوف نتعرف على طريقة الدراسة من خلال تحديد مجتمع وعينة الدراسة، وتحديد المتغيرات.

الفرع الأول :مجتمع وحجم عينة الدراسة:

أولاً: مجتمع الدراسة:

يتمثل مجتمع دراستنا في المؤسسات العاملة في مختلف قطاعات في ولاية ورقلة و تم اختيار مؤسسة اتصالات الجزائر - المديرية الجهوية للاتصالات بورقلة- كونها رائدة في مجال الاتصالات وبالتالي تتضمن جميع الوسائل المتعلقة بنظام معلومات إلكتروني كما وقع الاختيار على شركة سونلغاز كمجتمع دراسة، بما تعتبر بيئة تطبيقية تتناسب مع الدراسة ، مما يتيح له سهولة

الحصول على المعلومات وبإضافة إلى مؤسستين الكبيرتين ولتوسيع دراسة وإمكانية المقارنة الفعالة قمنا باختيار مجتمع لدراسة ثالث وهي مؤسسة ليند غاز

ثانيا :حجم العينة الدراسة :

وكان حجم العينة الدراسة حسب معادلة ستيفن ثامبسون:

$$n = \frac{N \times p(1-p)}{\left[\left[N-1 \times (d^2 \div z^2) \right] + p(1-p) \right]}$$

حيث أن :

p : نسبة توفر الخاصية والمحايدة = 0.50

N : حجم المجتمع

Z : لدرجة المعيارية المقابلة لمستوى الدلالة 0.95 وتساوي 1.96

d : نسبة الخطأ وتساوي 0.05

وبناء على المعلومات المجمعة من طرف الطالب على المقابلة مع المسؤولين المؤسسات محل الدراسة وكانت المعلومات كالآتي :

✓ مجتمع من مستخدمي نظام المعلومات في المؤسسة سونلغاز ورقلة يقدر 100مستخدم وبعد تطبيق معادلة ستيفن ثامبسون نجد 79مستخدم .

✓ مجتمع من مستخدمي نظام المعلومات في المؤسسة اتصالات الجزائر ورقلة يقدر 150مستخدم وبعد تطبيق معادلة ستيفن ثامبسون نجد 108مستخدم.

✓ مجتمع من مستخدمي نظام المعلومات في المؤسسة ليند غاز ورقلة يقدر 18مستخدم وبعد تطبيق معادلة ستيفن ثامبسون نجد 17مستخدم.

ومن ما سبق أهمية من حساب حجم العينة بتطبيق معادلة ستيفن ثامبسون لكي لا تقل العينة عن هذا الحجم وتعطي صورة شاملة وحقيقية وبناء على هذا الحجم تم توزيع الاستبان على مستخدمين ومشرفون تابعين لمؤسسات محل الدراسة ليشمل العينة الموضحة في الجدول (2-1) كما يلي:

الجدول (1-2): الاستثمارات الموزعة على الشركات محل الدراسة

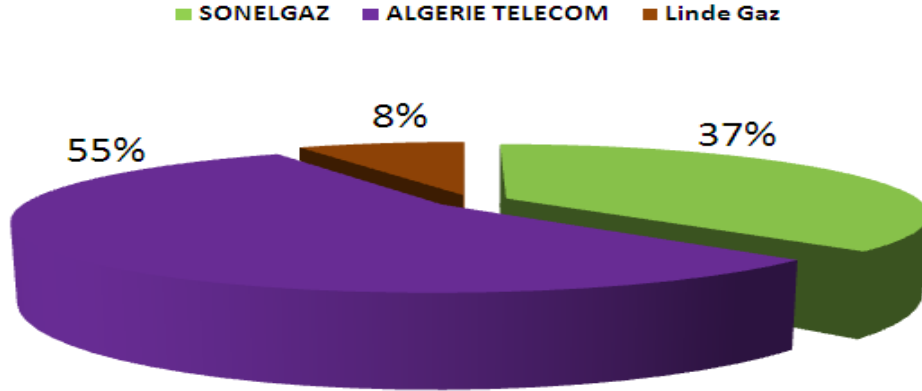
مستخدمي النظام			المشرفون على النظام			إجمالي الاستبيان			المؤسسة
الملغاة	المسترجعة	الاستبيانات الموزعة	الملغاة	المسترجعة	الاستبيانات الموزعة	الملغاة	المسترجعة	الاستبيانات الموزعة	
05	70	75	00	10	10	05	80	85	SONELGAZ
05	105	110	00	15	15	05	120	125	ALGERIE TELECOM
00	17	17	00	01	01	00	18	18	Linde Gaz

المصدر: من إعداد الطالب بناء على نتائج المقابلة ونتائج توزيع الاستبيان

ومن أجل معرفة نسبة مئوية مساهمة كل مؤسسة محل الدراسة في العينة الدراسة إلى إجمالي العينة كما هو موضح في الشكل

الآتي :

الشكل (1-2): توزيع الاستثمارات الموزعة على الشركات محل الدراسة



المصدر: من إعداد الطالب بناء على نتائج المقابلة ونتائج توزيع الاستبيان

ومن الشكل أعلاه وبمقارنة نسبة كل مؤسسة إلى إجمالي العينة نجد ان مؤسسة اتصالات اكبر نسبة 55% تقدر 120 الاستبيان و ثم مؤسسة سونلغاز بنسبة 37% والمقدرة ب 80 استبيان وتليها مؤسسة ليند غاز بنسبة 8% والتي تقدر 18 استبيان وهذا راجع على صغر وقلة مستخدمي النظام ومشرفون لوحدة ورقلة ولكن على مستوى فردي إي نسبة العينة مستخدمة في الدراسة إلى العمال الإجمالي لكل مؤسسة وحيدة تتصدر ليند غاز بنسبة 100% المقدر ب 18 مستخدم ومشرف.

الفرع الثاني :تعريف المؤسسات محل الدراسة :

الجدول (2-2) : تعريف عينة الدراسة

الرقم	اسم المؤسسة	نوع نشاط	إطار قانوني	المرسوم	تاريخ التأسيس
01	الشركة الوطنية للكهرباء والغاز SONELGAZ	نشاطات إنتاج ونقل وتوزيع الكهرباء والغاز	شركة مساهمة تملك الدولة رأسمالها	1969-59	28 جويلية 1969
02	اتصالات الجزائر ALGERIE TELECOM	تنشط في سوق شبكات وخدمات الاتصالات الإلكترونية	مؤسسة ذات أسهم	2000-03	05 أوت 2000
03	ليند غاز Linde Gaz Algérie	إنتاج وتوزيع مختلف الغازات الصناعية والطبية	شراكة الجزائرية 34%-الألمانية 66%	1983-32	01 جانفي 1983

المصدر: إعداد الطالب اعتمادا على معلومات من المؤسسات محل الدراسة

المطلب الثاني : الأدوات المستخدمة الدراسة :

يشمل هذا المطلب استعراض الأدوات المستخدمة في جمع المعلومات، وكذلك البرامج والأدوات الإحصائية المستعملة في تحليل المعطيات المتحصل عليها من خلال عملية توزيع الاستبيان على عينة الدراسة.

الفرع الأول : الأدوات المستخدمة في الدراسة :

خلال هذا البحث تم الاعتماد على أدوات البحث التالية :

أولاً: المقابلة : تعتبر المقابلة الأداة الرئيسية التي ارتكزت عليها دراستنا في جمع المعلومات حيث إننا وضعنا برنامج لإجراء المقابلات مع مدير وإطارات نظام المعلومات ، وكان هذه المقابلة يتمحور حول مكونات وعناصر نظام المعلومات الالكتروني والسياسات الأمنية المتبعة في المؤسسات محل الدراسة ، و إضافة إلى جمع المعلومات المتعلقة بالإدارة المشرفة على نظام المعلومات والمعلوماتية في المؤسسة، أما بالنسبة للأسئلة المستخدمة في المقابلة فقد تم صياغة شاملة كما وفيكما هو موضح في الملحق رقم(01)

ثانياً: الملاحظة : من أجل تقرب أكثر على واقع نظام المعلومات داخل المؤسسة ، والوقوف مباشرة على سير عمل خلالها ، استعملنا الملاحظة من خلال التواجد في مختلف المصالح ومراقبة البرامج ووسائل الشبكة ، وطريقة تعامل الموظفين فيما بينهم .

ثالثا: الاستبيان: استخدمنا الاستبيان كأداة من أدوات جمع البيانات الأولية اللازمة، لما للاستبيان من أهمية في توفير الوقت والجهد علينا ، حيث تم تصميمه ليتم توجيهه إلى الإطارات والموظفين العاملين في إدارة المعلوماتية ، للوقوف على مدى تأثير امن نظم المعلومات على المخاطر نظم المعلومات .
ولقد تم بناء وتطوير الاستبيان بالاعتماد على الإطار النظري للدراسة وعلى ضوء المراجعة الشاملة للدراسات السابقة، التي تناولت موضوع امن الكتروني ومخاطر نظم المعلومات (ذات الصلة بالموضوع)، كما تم الاستعانة بآراء بعض الأساتذة الجامعيين وبعض الموظفين في المؤسسات ، كما هو موضح في الملحق رقم(02)

أ- بناء الاستبيان: تم تقسيم الاستبيان إلى ثلاثة محاور رئيسية كما يلي:

المحور الأول المعلومات العامة: ويتضمن المعلومات الشخصية والمتكون من 08 فقرات.

المحور الثاني مخاطر نظم المعلومات: ويتضمن المخاطر المتعلقة بالمكونات والعناصر نظم المعلومات ويحتوي على 14 فقرة

وقد كانت الإجابات على فقرات هذا المحور " لم يحدث أبدا " " أحيانا " " يحدث دائما"

المحور الثالث نظام الأمن الكتروني في المؤسسة: وتم تقسيمه إلى ثلاثة الأبعاد:

البعد الأول السياسات والإجراءات يحتوي على 11 فقرة ، أما **البعد الثاني** إجراءات امن المعلومات المتعلقة بالعاملين يحتوي على 7 فقرات ، وتكون **البعد الثالث** إجراءات امن المعلومات المتعلقة بالعتاد والبيانات ويحتوي على 10 فقرات وام بالنسبة للإجابات على فقرات هذا المحور " غير موافق " " محايد " " موافق "

المطلب الثالث : تحليل واقع النظام الأمن الكتروني في المؤسسة :

سنتناول في هذا المطلب واقع النظام الأمن الكتروني في المؤسسات محل الدراسة والتي تم جمع المعلومات بأدوات سألها ذكر من اجل اعطى صورة حقيقية تمثل الواقع الحقيقي للأمن الكتروني والنظم المعلومات والسياسات الأمنية المتبعة وتم تقسيم المطلب أعلاه إلى فرعين هما :

الفرع الأول :مكونات نظام معلومات المؤسسة :

بناء على المقابلة والملاحظة تم تجميع المعلومات التالية : يتكون نظام معلومات من الأجهزة و المعدات، البرمجيات، العنصر البشري، قاعدة البيانات والشبكات.

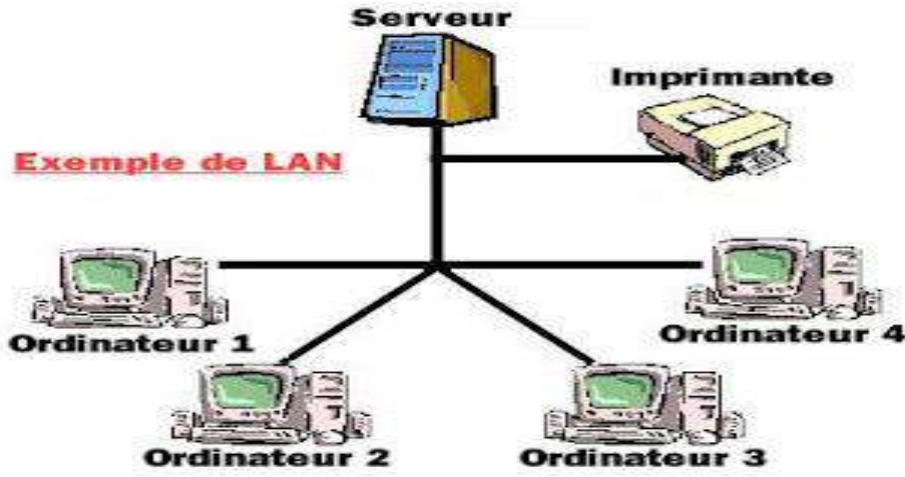
يبين الشكل السابق تمثيل لتقنية خادم/زبون، حيث يتواجد مركزيا خادم واحد أو مجموعة من الخوادم، ترتبط مع أجهزة تسمى زبائن، قد يكون هذا الزبون محطة طرفية، أو حاسوب محمول، أو طابعة... الخ.

أولا : مؤسسة سونلغاز :

01 :الأفراد :

ينقسم العنصر البشري إلى شقين ، الشق الأول وهم الأشخاص المسؤولين على تسيير نظام المعلومات ، والشق الثاني يضم الأشخاص المستغلين لهذا النظام (المستخدممي النظام) ويعتمد على تقنية خادم/زبون كما هو مبين في الشكل التالي:

الشكل (2-2): تقنية خادم/ زبون



المصدر : مصلحة الإعلام الآلي

أشخاص الدعم : وهم التعداد المسؤول على صيانة وضمان السير الحسن لنظام المعلومات وعددهم يختلف من مؤسسة إلى أخرى موزعين حسب الجدول التالي:

الجدول(2-3):توزيع موظفي نظام المعلومات لمؤسسة سونلغاز

numéro	Qualification	Quantité
01	Ingénieur d'Etat en électronique	02
02	Ingénieur d'Etat en informatique	05
03	technicien supérieur en informatique	01
04	technicien supérieur en communications	04

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس مصلحة المعلوماتية

02: العتاد والاجهزة الكترونية :

أ- الوصف المكاني : تقع مصلحة نظام المعلوماتية في الطابق الأول كما أن الأجهزة موضوعة في مكتب كبير يمنع الدخول له إلا للضرورة القصوى وهذا المكتب مقسم إلى قسمين القسم الأول للمشرفون على النظام والقسم الثاني الأجهزة والعتاد .

ب- الأجهزة والعتاد الكتروني : يتكون النظام من مجموعة أجهزة مبينة في الجدول التالي :

الجدول(2-4): الأجهزة الكترونية لنظام المعلومات مؤسسة سونلغاز

numéro	Equipement	Marque	Quantité
01	Micro ordinateur Optiplex 9020 500 Go INTEL 2.5 GHZ	Dell	04
02	Micro ordinateur LCD 500 Go INTEL 1.5 GHZ	Condor	09
03	Onduleur UPS Périph	APC	12
04	Server Data Base Power Edge 500 To 12 Processeur	Dell	02
05	Server Data Base Power Edge 500 To 24 Processeur	Dell	04
06	Modem 5	Cisco	05
07	Switch Périph	Cisco	22
08	Routeur Périph	Cisco	04
09	imprimante MS510 DN	LEXMARC K	05
10	imprimante B411 DN	OKI	01
11	imprimante ML3710 ND	SAMSUNG	01
12	Caméra de surveillance	SONY	04
13	Capteurs d'incendie	/	/
14	Capteurs d'incendie	/	/
13	Climatiseur 18000	Condor	02

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس مصلحة المعلوماتية

مكونات نظام المعلومات الإلكتروني، حيث تسمح بتشغيل النظام من خلال تسيير مختلف التطبيقات المعلوماتية بواسطة شبكة الاتصال للوصول لقواعد البيانات قصد تخزين أو استرجاع المعلومات الأجهزة الإلكترونية المستخدمة في مصلحة تسيير وتطوير نظام المعلومات الإلكترونية الخاصة بالمؤسسة.

03 قاعدة البيانات :

تتكون قواعد البيانات الخاصة بنظام المعلومات من أربعة خوادم قاعدة بيانات من نوع "Dell" وتتبع للصف Power Edge" بسعة 500 تيرا أوكتي و 24 معالج مدعومة بخادمين احتياطيين من نوع "Dell" وتتبع للصف "Power Edge" بسعة 500 تيرا أوكتي و 12 معالج، كما تستخدم تقنية التخزين المزدوج في تخزين معلومات قاعدة المعطيات، ونوع هيكل قاعدة البيانات هو الهيكل الشبكي للبيانات Network Data Structure.

04 البرامج المستخدمة :

البرنامج المستعمل في إنشاء قاعدة البيانات هو ORACLE واللغة الاستعلامية لقواعد البيانات 2014 Sql Server ويعمل الخادم بنظام التشغيل Windows server
✓ "SGC" نظام معلومات تسيير الزبائن.
✓ "NOVA" نظام معلومات تسيير الموارد البشرية.
✓ "HISSAB" نظام معلومات مالي محاسبي انظر الملحق (03)

05 : الشبكات :

- شبكة الاتصالات الإلكترونية : يتم الاتصال بالشبكة الواسعة "WAN" للوصول لقواعد البيانات في الجزائر العاصمة من خلال شبكة شركة اتصالات الجزائر من نوع "HDSL"
- تقنية اتصال داخلي: "Kerio Connect": هي تقنية اتصال تستخدم في إرسال الملفات ما بين رئيس القسم ومختلف مسؤوليه وتكون في شكل تقارير ولوائح تنظيمية وتعليمات واردة وصادرة، ذات صلة بمخرجات نظام المعلومات أو بمدخلاته انظر الملحق (04)
- تقنية اتصال داخلي: "TENSİK" : هي تقنية اتصال إلكتروني من تصميم "ELIT" تعمل من خلال الاتصال يربط بين شركات وفروع فيما بينها انظر الملحق (05)

ثانيا :مؤسسة اتصالات الجزائر :

01 :الأفراد : ينقسم العنصر البشري إلى شقين ، الشق الأول وهم الأشخاص المسؤولين على تسيير نظام المعلومات ، والشق الثاني يضم الأشخاص المستغلين لهذا النظام (المستخدممي النظام).

أشخاص الدعم : وهم التعداد المسؤول على صيانة وضمان السير الحسن لنظام المعلومات وعددهم حسب الجدول التالي:

الجدول(2-5):توزيع موظفي نظام المعلومات لمؤسسة اتصالات الجزائر

numéro	Qualification	Quantité
01	Ingénieur d'Etat en électronique	01
02	Ingénieur d'Etat en informatique	03
03	technicien supérieur en informatique	03
04	technicien supérieur en communications	03
05	majesteur en informatique	03
06	Lissanse en communications	02

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس المصلحة

يتضح من خلال الجدول أعلاه، أن العنصر البشري الذي يسهر على سير نظام المعلومات ذو تكوين عالي في في المؤسسة ، وهذا دليل على أهمية نظام المعلومات .

✓ الأشخاص المستغلون لنظام التشغيل: وهم جميع العمال في وكالات تجارية والمصالح التقنية والإدارية.

02: العتاد والاجهزة الكترونية :

أ-الوصف المكاني : تقع المصلحة في الطابق الثاني، في بناية وسط المدينة، وهي أعلى طابق في البناية، ويمنع الوصول لأي شخص غريب عن المصلحة لتلك البناية، كما أن الأجهزة موضوعة في مكان زجاجي شفاف، ويمنع دخولها إلا للضرورة القصوى.

ب -الأجهزة والعتاد الكتروني : يتكون النظام من مجموعة أجهزة مبينة في الجدول التالي :

الجدول(2-6):الأجهزة الكترونية لنظام المعلومات مؤسسة اتصالات الجزائر

numéro	Equipement	Marque	Quantité
01	Micro ordinateur	HP	02
02	Firewall	Stonesoft	02
03	Onduleur 40KVA	/	02
04	Server Data 08 Processeur 15TB	BULL	05
05	générateur d'électricité	/	01
06	Switch Périph	Cisco	22
07	Routeur Périph	Cisco	02
08	imprimante	HP	04
09	Stockage externe automatisé Robot chez les femmes enceintes	/	01
10	Caméra de surveillance	/	01
11	Climatiseur 50000	SAMSUNG	02
12	Climatiseur 18000	LG	02

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس المصلحة

حيث يسمح هذا العتاد بتشغيل النظام من خلال تسيير مختلف التطبيقات المعلوماتية بواسطة شبكة الاتصال للوصول لقواعد البيانات قصد تخزين أو استرجاع المعلومات .

03 قاعدة البيانات :

بنيت قواعد المعطيات لنظام المعلومات بقواعد المعطيات أوراكل وهو نظام قوي، كما يقبل لغة البرمجة الاستعلامية، التي تسمح بمحاورة قواعد المعطيات بسلاسة.

04:البرامج المستخدمة :

يحتوي النظام على نوعين من البرامج، برنامج التشغيل (نظام التشغيل)، ونظام التسيير وهما:

أ- نظام التشغيل : تشتغل الخادماات في بيئة UNIX بنسخة Aix 5.3 UNIX

ب- برنامج نظام المعلومات قايا : هو نظام معلومات مطور من طرف شركة سوفريكوم الفرنسية، موجه خصيصا إلى المتعاملين في ميدان الاتصالات، حيث يسمح بتسيير الجانب التجاري والتقني للزبائن، استثمرت اتصالات الجزائر في هذا

النظام منذ 2004، وهو مازال مستمر ولكن تم تطويره من قايا 05 الى قايا 07 وعلى مستوى المركزي في العاصمة لا على مستوى الجهوية التي تم تحويلها الى مديرية ولائية مع تغييرات الجديدة 2017، انظر الملحق (06)

ويمتاز برنامج قايا بعدديد من المزايا وخصائص ونذكر منها :

- ✓ قراءة آلية لملفات التحصيل؛
- ✓ تحميل معطيات خارجية في ملفات النظام؛
- ✓ وسيط تحويل من محاسبة الزبائن إلى المحاسبة العامة في برامج أخرى كأوراكل؛
- ✓ وسيط الدفع مع الهيئات البنكية الأخرى؛
- ✓ وسيط تحويل البيانات نحو معدي دليل الهاتف؛
- ✓ وسيط نحو وسائل إعداد التقارير البيانية.

05: الشبكات:

تعتبر الشبكات من بين أهم عناصر نجاح نظام المعلومات كونها تسمح للزبائن بالاتصال بالخوادم المركزية، وتتوفر اتصالات الجزائر بحكم طبيعة نشاطها على مجموعة مختلفة من الشبكات التي تدعم نظام المعلومات:

➤ شبكة RMS

➤ شبكة LAN

➤ شبكة VPN

➤ شبكات X25

ثالثا: مؤسسة ليند غاز :

01: الأفراد : ينقسم العنصر البشري إلى شقين ، الشق الأول وهم الأشخاص المسؤولين على تسيير نظام المعلومات ، والشق الثاني يضم الأشخاص المستغلين لهذا النظام (المستخدممي النظام).

أشخاص الدعم : وهم التعداد المسؤول على صيانة وضمان السير الحسن لنظام المعلومات وعددهم يختلف من مؤسسة إلى أخرى موزعين حسب الجدول التالي:

الجدول(2-7):توزيع موظفي نظام المعلومات لمؤسسة ليند غاز

numéro	Qualification	Quantité
01	Ingénieur d'Etat en informatique	01

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس مصلحة إعلام الآلي

02: العتاد والاجهزة الكترونية :

أ - الوصف المكاني : تقع غرفة الأجهزة في الطابق الأول فوق مصلحة الإعلام الآلي وهي عبارة عن غرفة صغيرة يحاط عليه جدار نصفه اسمنت والباقي زجاج تفتقر إلى المراقبة الإلية ويمنع دخول لها عدا المهندس المشرف على نظام المعلومات المؤسسة انظر الملحق (09) .

ب - الأجهزة والعتاد الكتروني : يتكون النظام من مجموعة أجهزة مبينة في الجدول التالي :

الجدول(2-8):الأجهزة الكترونية لنظام المعلومات مؤسسة ليند غاز

numéro	Equipement	Marque	Quantité
01	Micro ordinateur	HP	01
02	Firewall+ Routeur Périph	Cisco	02
03	Onduleur 20KVA	AEK	01
04	Server Data 08 Processeur 1. 5TB Tri par défaut	Microsoft	05
05	générateur d'électricité	/	01
06	Switch Périph	Cisco	24
07	imprimante	CANON	06
08	Climatiseur 12000	SAMSUNG	02

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع رئيس مصلحة إعلام الآلي

03: قاعدة البيانات :

تتكون قاعدة بيانات المؤسسة للنظام معلومات من خادم من نوع Microsoft بسعة صغيرة تقدر ب1.5 تيرا ولكن كافية لتخزين معلومات الوحدة وبدورها تنقل المعلومات لتخزينها على مستوى الجزائر العاصمة وهذا الخادم تم تقسيمه إلى خادم ثلاثي افتراضية ودورها كما يلي:

- أ- **نقطة توزيع**: تحتوي على البرامج وتحديثات ومضادات الفيروسات المرخصة فقط من طرف الشركة لإلام
- ب- **نقطة طباعة**: يحسب ويخزن كل أوامر طباعة ومعرفة أي ورقة تم طباعها وهذه طريقة من اجل تسهيل عملية تدقيق و المراقبة ومن اجل تقليل عملية طباعة ورق لحفاظ على البئية.
- ج- **نقطة الثالثة**: هو عبارة على نقطة افتراضية من اجل متابعة قارورات الغاز معبأة أو فارغة.

04: البرامج المستخدمة :

- يحتوي نظام المعلومات المؤسسة على ثلاثة البرامج وهي كالآتي:
- ✓ ERP Microsoft : برنامج عالمي ومتطور مصمم على الحجم واحتياجات المؤسسة ويسير كل مصالح ماعدا الرواتب والأجور التي تم حذفها من البرنامج بسبب ما تتميز به الجزائر من تعقيد وعدم ملائمة الرواتب واشتراكات الجبائية وشبه جبائية.
 - ✓ سياج : برنامج تسيير الأجور والرواتب .
 - ✓ التراكيث : برنامج خاص بمتابعة قارورات الغاز الفارغة ومعبأة .

05 : الشبكات :

- يحتوي النظام المعلومات المؤسسة على ثلاثة شبكات من أجل تجنب الأعطال وتعطل اتصال الوحدة بالشركة الأم وهي كالآتي:
- ❖ خط خاص بين وحدة ورقلة والشركة الأم والبديل الثاني عند تعطل الشبكة الأولى يوجد ADSL ثم بديل ثالث استعانة بشبكة القمر الصناعي التي مؤسسة مشتركة فيه مع مؤسسة خاصة

الفرع الثاني : السياسات الأمنية المتبعة :

يعد اعتماد الإجراءات والاحترازمات الأمنية، أمراً حتمياً لحماية نظم المعلومات الإلكترونية، لما له من أهمية في الحفاظ على سلامة المعلومات ، إذ تعتبر جزء مهما لاستفءاء كل معلومات مؤسسة ، حيث يرتبط أمن النظام وسلامة المعلومة ، بثقة المؤسسة في اتخاذ القرار سليم ، وإمكانية الاعتماد عليها، على هذا الأساس تعتمد كل المؤسسات على السياسات الأمنية على مستوى الأفراد وعتادها.... الخ للحماية نظام معلوماتها ومكوناته وهي كالآتي:

أولا : سونلغاز :

- ✓ استعمال التخزين المزدوج لمعطيات قواعد البيانات، وحفظ مخرجات نظام المعلومات في نسخ إلكترونية احتياطية.

الفصل الثاني: الدراسة الميدانية لتقييم اثر الالكتروني في الحد من المخاطر النظم المعلومات

- ✓ طباعة آلية لاسم المستخدم على مخرجات كل عملية إدخال ، سواء كان إدخال يدوي أو آلي، بما يحقق الأثر في تسجيل أي عملية وعدم الإنكار، ويجسد الرقابة على المدخلات وتحديد مسؤولية كل مستخدم؛
- ✓ منع استعمال البرامج ومضادات الفيروسات الغير مرخصة؛
- ✓ إرساء ثقافة المؤسسة من خلال التحلي بالأمانة في تسيير الموارد المالية، والتأكيد على حفظ السر المهني والحفاظة على الملفات والمستندات المحاسبية، كأثر مادي لأحداث الشركة؛
- ✓ منع إيصال الكمبيوتر المحمول الشخصي بشبكة الاتصال الداخلي للمؤسسة؛
- ✓ دورات تدريبية خاصة بالأمن بإشراف المهندس المكلف بالأمن الصناعي، فيما يخص إجراءات السلامة لتشغيل وتوقيف الأجهزة الإلكترونية لنظام المعلومات؛
- ✓ تخصيص كلمة سر لكل مستخدم للنظام، كما هو موضح في الملحق رقم 02
- ✓ الصيانة الدورية للعتاد من طرف مهندسين مختصين في الصيانة؛
- ✓ تخصيص خزانة فولاذية لحفظ الشيكات والضمانات البنكية للتنفيذ كودائع لآجال والملفات المهمة ونسخ الكترونية ، مقبوضة من الموردين؛
- ✓ تثبيت أربعة كاميرات للمراقبة، لمنع دخول الأشخاص الغير مرخص لهم بالدخول إلى أماكن تواجد الخوادم والأجهزة الإلكترونية ذات العلاقة بأمن المعلومات؛
- ✓ التشديد على أهمية عملية الأرشيف للمستند المحاسبي، والحرص على تنظيمه وحمايته، من خلال تخصيص قاعة لأرشيف خاصة ببعض الأقسام المهمة ، غير مخول للأشخاص الآخرين الدخول لها؛
- ✓ استخدام جدار ناري قائم على جهاز متخصص من نوع "Firewall Hardware"

ثانيا : اتصالات الجزائر :

- ✓ موقع وجود خادما ت قواعد البيانات استراتيجي ، ويمنع أي شخص غريب عن المصلحة للدخول إليه؛
- ✓ تحتوي البناية على مصعد كهربائي خاص بالأجهزة؛
- ✓ قاعة الخوادم ، في حيز زجاجي ، مما يمكن أي شخص مسؤول أن يلحظ أي تحذير؛
- ✓ توفير تكييف جيد مع وجود مولدات للكهرباء؛
- ✓ وجود مضادات الحرائق.
- ✓ طاقم مشرف على النظام عالي التكوين ويستفيد من تكوينات دورية؛
- ✓ يحصل كل عامل على تكوين متخصص في ميدان عمله (تجاري ، مالي ، تقني)؛
- ✓ كل عامل يستغل نظام المعلومات قايًا ، يحصل على كلمة سر واسم مستعمل خاص به و نموذج خاص به؛
- ✓ كل عملية تحدث على مستوى النظام تسجل باسم العامل الذي قام بها.
- ✓ شبكة محلية موجودة ترتبط بالخوادم عن طريق بروتوكلين TCP/IP و X25؛
- ✓ خوادم عالية الأداء وذات سرعة فائقة؛
- ✓ ملحقات كشف الحريق والتبريد الملائم وتأمين التيار الكهربائي في حال الانقطاع متوفرة؛

- ✓ الحواسيب النهائية (الزبائن) مختلفة ومن أجيال متقاربة، ، أداءها مقبول، مخزونات الطاقة متوفرة وليست كافية؛
- ✓ أجهزة اتصال، هاتف، فاكس متوفرة وتستهمل أحيانا؛
- ✓ الطابعات متوفرة سواء كانت مركزية أو شخصية.
- ✓ نسخ احتياطي يومي وشهري، النسخ الشهري يتم في حوامل خارجية وتحفظ في مكتب المدير وهناك حفظ تزامني يحدث مرة في الشهر مع قواعد معطيات على مستوى العاصمة؛
- ✓ وجود نسخ احتياطية لقاعدة معطيات العاصمة في جميع الوحدات التابعة لها؛
- ✓ مضاد الفيروسات متوفر و متداخل مع الجدار الناري؛
- ✓ يتم إنشاء حسابات الزبائن من طرف شخص واحد مسؤول، حيث ينشأ لكل عامل اسم مستعمل، كلمة مرور وعنوان الحاسوب IP، وتخصيص معين؛
- ✓ يتم غلق كل حساب غير نشط مدة شهرين آليا؛
- ✓ برنامج تسيير قواعد البيانات عالي الأداء، وكذلك الحال لنظام التشغيل، البرنامج الرئيسي عبارة عن مجموعة مترابطة من الوحدات؛
- ✓ يعتبر الوصول إلى النظام عن طريق التالنت من أقوى نقاط قوة السياسات الأمنية حيث أن الزبون لا يملك تطبيق ، وإنما مجرد اتصال والتطبيق يفتح وينفذ على مستوى الخادم الرئيسي؛
- ✓ في حال ضرر يصيب الخادم الرئيسي تنتقل المراقبة أليا للخادم المرافق (الخاص بقاعدة) البيانات ليعوض الخادم المعطل، والعكس صحيح.
- ✓ الاتصال بنظام قايا يتم على طريق بروتوكول تالنت.
- ✓ أنظمة التشغيل ويندوز من نسخ مختلفة منها الأصلية ومنها غير أصلية؛
- ✓ مضاد فيروسات مركزي مثبت في أغلب الحواسيب؛
- ✓ اتصال انترنت متوفر وبثلاث أشكال وفي، شبكة، وأدي أس أل؛
- ✓ برامج مختلفة لأغراض متفرقة، عملية وشخصية؛

ثالثا: مؤسسة ليند غاز :

- ✓ توفير تكييف جيد حفاظ على الأجهزة؛
- ✓ وجود مولدات للكهرباء من اجل القضاء على انقطاع الطاقة
- ✓ مضاد فيروسات مركزي مرخص مثبت في أغلب الحواسيب؛
- ✓ تسجيل وتميز ببطاقة الزائر أي شخص غريب على الشركة وتسجيل اسمه والغرض من الزيارة ؛
- ✓ أجهزة اتصال، هاتف، فاكس متوفرة وتستهمل أحيانا؛
- ✓ أنظمة التشغيل ويندوز من نسخ مختلفة الأصلية فقط؛
- ✓ موقع وجود خادمت قواعد البيانات استراتيجي وبعيدة على متناول الجميع ؛
- ✓ الطابعات متوفرة سواء كانت مركزية أو شخصية ويقوم الخادم بتسجيل إي عملية طباعة .
- ✓ ويمنع أي شخص غريب عن المصلحة للدخول إلى القاعة الأجهزة ؛

- ✓ مؤسسة برنامج خاص اسمه "عنكبوت Spider" يخول لمهندس دخول ومعرفة أي تعديل جديد في وحدة تابعة لمؤسسة الأم.
- ✓ تتوفر المؤسسة على إجراءات الأمنية مكتوبة انظر الملحق (07)؛
- ✓ يحصل كل عامل على تكوين متخصص في ميدان عمله
- ✓ يتم غلق كل حساب غير نشط مدة 03 أشهر آليا؛
- ✓ يتم تحديث وتجديد كلمة السر لمدة 03 أشهر آليا من طرف شركة الأم وإرسال تقرير إلى ألمانيا ؛
- ✓ منع إدخال إي ذاكرة أو جهاز أو كابل إلى الشبكة أو جهاز وان حدث آليا يتم رفض ويتم تصريح إلى مؤسسة الأم ويفتح تحقيق؛
- ✓ في حال ضرر يصيب الخادم الرئيسي تنتقل المراقبة أليا للخادم المرافق (الخاص بقاعدة) البيانات ليعوض الخادم المعطل، والعكس صحيح.
- ✓ في حال تعطل احد الخوادم ينتقل العمل لخادم الافتراضي الثاني أو ثالث
- ✓ اتصال انترنت متوفر وبثلاث أشكال وفي، شبكة، وأدي أس أل والقمر الصناعي ؛
- ✓ وجود نسخ احتياطية لقاعدة معطيات العاصمة في جميع الوحدات التابعة لها وفي المجمع في ألمانيا ؛
- ✓ استخدام جدار ناري مع موجه قائم على جهاز متخصص من نوع "Cisco"

المبحث الثاني: النتائج المتحصل عليها ومناقشتها

المطلب الاول: النتائج الاستبيان

تم استخدام مجموعة من الأدوات الإحصائية من أجل القيام بدراسة وتحليل أجوبة عينة الدراسة حول مساهمة الأمن الكتروني في الحد من المخاطر في مؤسسات محل الدراسة ، وتشمل مجموعة من القياسات الخاصة بالاستبيان و الأدوات الإحصائية المستخدمة في البحث ما يلي:

الفرع الاول : الطريقة المستخدمة في القياس:

أولاً: مقياس ليكارت (Likert) الثلاثي: تم الاعتماد على مقياس ليكارت (Likert) الثلاثي، المكون من ثلاثة درجات لتحديد درجة أهمية كل سؤال من أسئلة الاستبيان، كما هو موضح في الجدول التالي:

الجدول (2-9): مقياس ليكارت الثلاثي المعتمد في الدراسة

يحدث دائماً	أحياناً	لم يحدث أبداً	المحور الثاني: مخاطر نظم المعلومات
موافق	محايد	غير موافق	المحور الثالث: نظام الأمن الكتروني في المؤسسة
03	02	01	درجة الوزن

المصدر: من إعداد الطالب

بعد تحديد مختلف الدرجات المتعلقة بأسئلة الاستبيان يتم بعد ذلك تحديد الاتجاه العام للإجابات من خلال المتوسط الحسابي المرجح، وذلك بالنظر إلى مجال وقوعه، كما هو موضح في الجدول التالي:

الجدول (2-10): المتوسطات المرجحة والاتجاه الموافق لها

يحدث دائماً	أحياناً	لم يحدث أبداً	المحور الثاني: مخاطر نظم المعلومات
موافق	محايد	غير موافق	المحور الثالث: نظام الأمن الكتروني في المؤسسة
3-2,34	2,33-1,66	1,66- 1	المتوسط المرجح

المصدر: من إعداد الطالب

ثانيا: مقياس ثبات آراء العينة الدراسة (ألفا كرونباخ):

يقصد بثبات الاستبيان أن يعطي هذا الاستبيان نفس النتيجة فيما لو تم إعادة توزيع الاستبيان أكثر من مرة تحت نفس الظروف والشروط، أو بعبارة أخرى إن ثبات الاستبيان يعني الاستقرار في نتائجه وعدم تغييرها بشكل كبير، فيما لو تم إعادة توزيع الاستبيان على أفراد العينة المبحوثة عدة مرات خلال فترات زمنية معينة.

وقد تحقق الطالب من ثبات استبيان الدراسة من خلال طريقة معامل الثبات "ألفا كرونباخ" كما هو موضح في الجدول اسفله:

الجدول (2-11): يوضح ثبات استمارة الاستبيان حسب معامل " ألفا كرونباخ"

المؤسسة	حجم العينة	عدد الفقرات	معامل ألفا كرونباخ	نسبة ألفا كرونباخ %
المؤسسة سونلغاز ورقلة	80	42	0,878	87.8
المؤسسة اتصالات الجزائر ورقلة	120	42	0,920	92
المؤسسة ليند غاز وحدة ورقلة	18	42	0,782	78.2

المصدر: من إعداد الطالب بناء على برنامج Spss

تبين القيم المتحصل عليها أنها مدى ثبات آراء العينة، حيث كانت جد مقبولة في المحمل المؤسسات وكانت قيمة المتوسط ألفا كرونباخ 0,86، وكانت نتائج اتصالات الجزائر أكبر ومقدرة 0,920 وهذا دليل على ثبات الإجابات الاستبيان ثم تاليها سونلغاز والتي لا تقل عنها بكثير حيث قدر المؤشر ب 0,878 وتأتي ليند غاز بمقدار الثبات 0,782 ويعتبر مقبول

الفرع الثاني: تحليل وصفي لخصائص الديمغرافية لعينة الدراسة

أولاً: توزيع أفراد حسب الجنس :

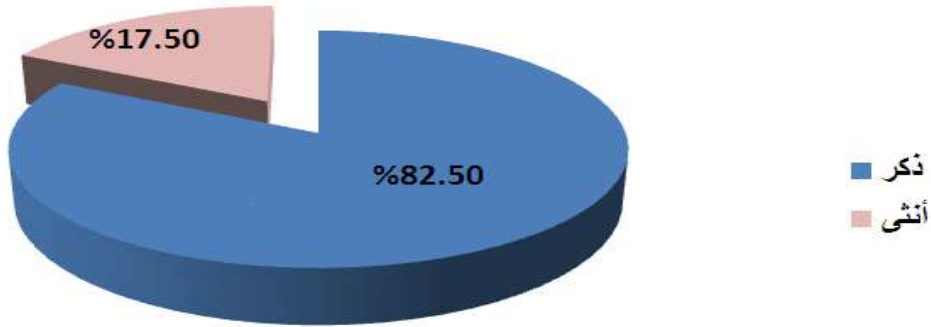
الجدول (2-12): توزيع حسب الجنس

البيان	سونلغاز		اتصالات الجزائر		ليند غاز	
	التكرار	النسبة %	التكرار	النسبة %	التكرار	النسبة %
ذكور	66	82,5	62	51,7	12	66,7
الإناث	14	17,5	58	48,3	06	33,3

المصدر: من إعداد الطالب بناء على برنامج Spss

01- مؤسسة سونلغاز :

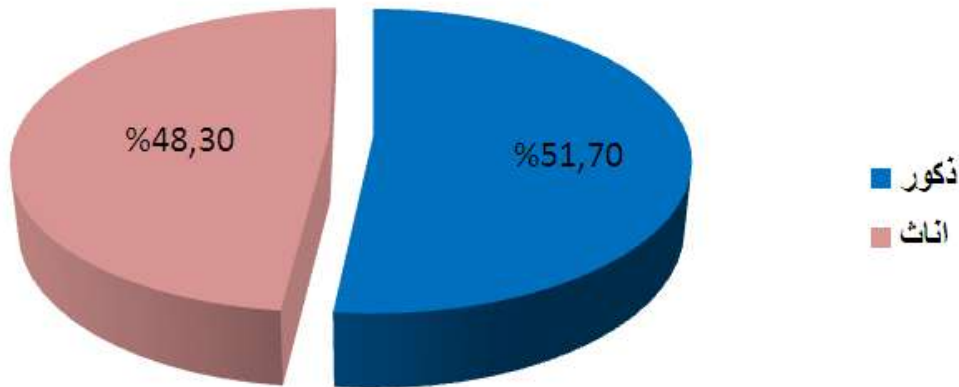
الشكل (2-3) : توزيع حسب الجنس لمؤسسة سونلغاز



المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة اتصالات الجزائر :

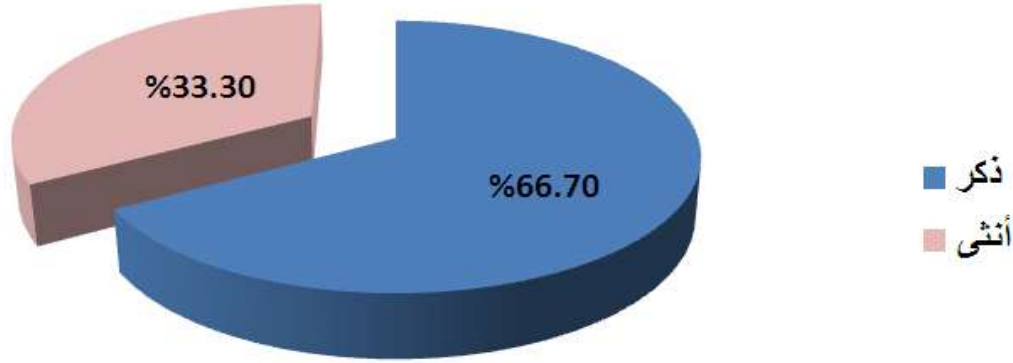
الشكل (2-4) : توزيع الأفراد حسب الجنس لمؤسسة اتصالات الجزائر



المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة ليند غاز:

الشكل (2-5) : توزيع حسب الجنس لمؤسسة ليند غاز



المصدر: من إعداد الطالب بناء على برنامج Spss

من خلال أشكال أعلاه تبين النتائج أن العينة كانت متكافئة إلى حد بعيد من حيث التوزيع حسب الجنس في مؤسسة اتصالات الجزائر، وكانت نسبة أكبر فئة ذكور في مؤسستي سونلغاز وليند غاز وهذا تفسيره طبيعة نشاط المؤسسة التي تكتسي طبيعة تقنية عكس مؤسسة اتصالات الجزائر خدمية

ثانيا: توزيع أفراد حسب الخبرة :

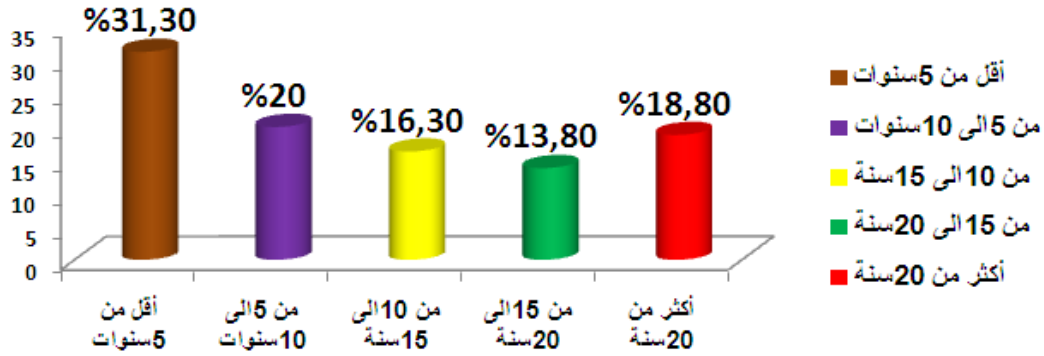
الجدول (2-13) : توزيع حسب الخبرة

ليند غاز		اتصالات الجزائر		سونلغاز		البيان
النسبة %	التكرار	النسبة %	التكرار	النسبة %	التكرار	
11,1	2	14,2	17	31,3	20	أقل من 5 سنوات
27,8	5	22,5	27	20,0	16	من 5 إلى 10 سنوات
27,8	5	35,0	42	16,3	13	من 10 إلى 15 سنة
11,1	2	15,8	19	13,8	11	من 15 إلى 20 سنة
22,2	4	12,5	15	18,8	15	أكثر من 20 سنة

المصدر: من إعداد الطالب بناء على برنامج Spss

01- مؤسسة سونلغاز:

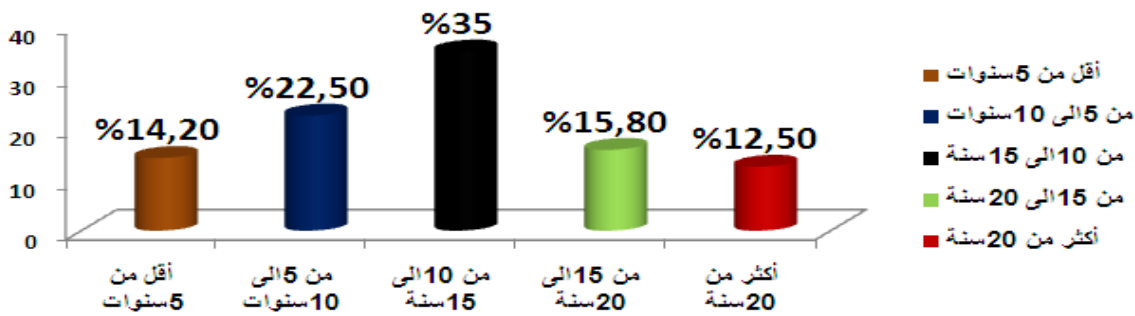
الشكل (2-6) : توزيع حسب الخبرة لمؤسسة سونلغاز



المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة اتصالات الجزائر:

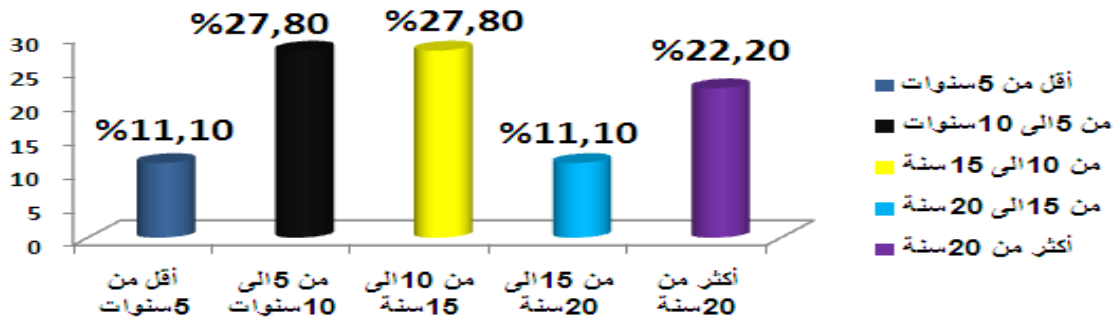
الشكل (2-7) : توزيع الأفراد حسب الخبرة لمؤسسة اتصالات الجزائر



المصدر: من إعداد الطالب بناء على برنامج Spss

03- مؤسسة ليند غاز:

الشكل (2-8) : توزيع حسب الخبرة لمؤسسة ليند غاز



المصدر: من إعداد الطالب بناء على برنامج Spss

يتضح لنا من خلال إشكال أعلاه أن نسبة أفراد العينة الذين لديهم الخبرة في مجال العمل ، الممتد من 05 سنوات إلى أكثر من 15 سنة بلغت تقريبا أكثر 50% في ، إذ يعد هذا مؤشرا إيجابيا على أن أفراد العينة من ذوي الخبرات العالية نسبيا، وهي خبرة كافية لتقييم نظام الأمن الكتروني ومساهمته في الحد من المخاطر نظم المعلومات.

ثالثا: توزيع أفراد حسب المؤهل العلمي :

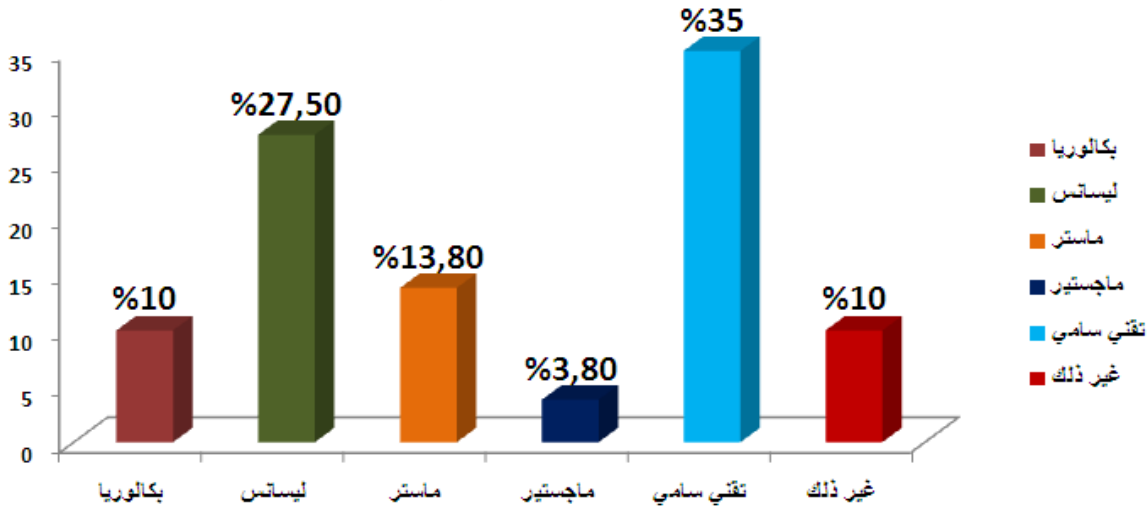
الجدول (2-14) : توزيع حسب المؤهل العلمي

البيان	سونلغاز		اتصالات الجزائر		ليند غاز	
	التكرار	النسبة %	التكرار	النسبة %	التكرار	النسبة %
بكالوريا	8	10,0	13	10,8	2	11,1
ليسانس	22	27,5	32	26,7	6	33,3
ماستر	11	13,8	15	12,5	2	11,1
ماجستير	3	3,8	5	4,2	1	5,6
تقني سامي	28	35,0	39	32,5	6	33,3
غير ذلك	8	10,0	16	13,3	1	5,6

المصدر: من إعداد الطالب بناء على برنامج Spss

01- مؤسسة سونلغاز:

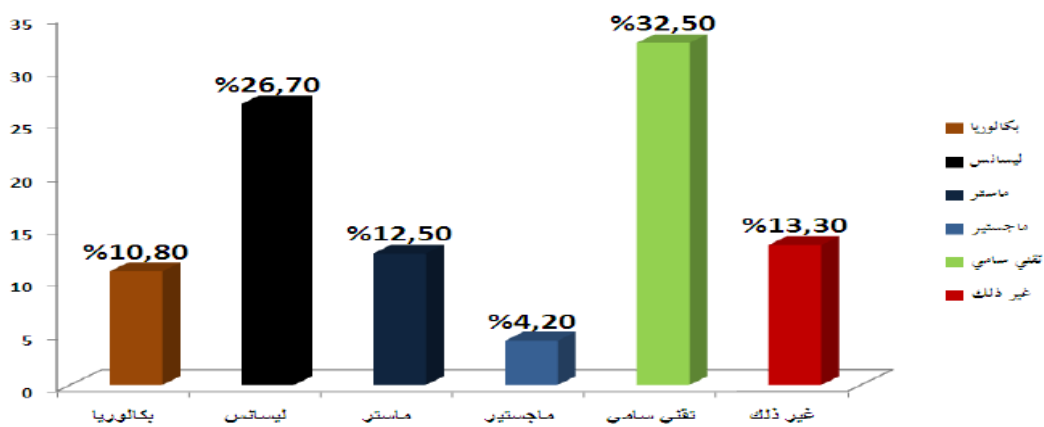
الشكل (2-9): توزيع حسب المؤهل العلمي لمؤسسة سونلغاز



المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة اتصالات الجزائر:

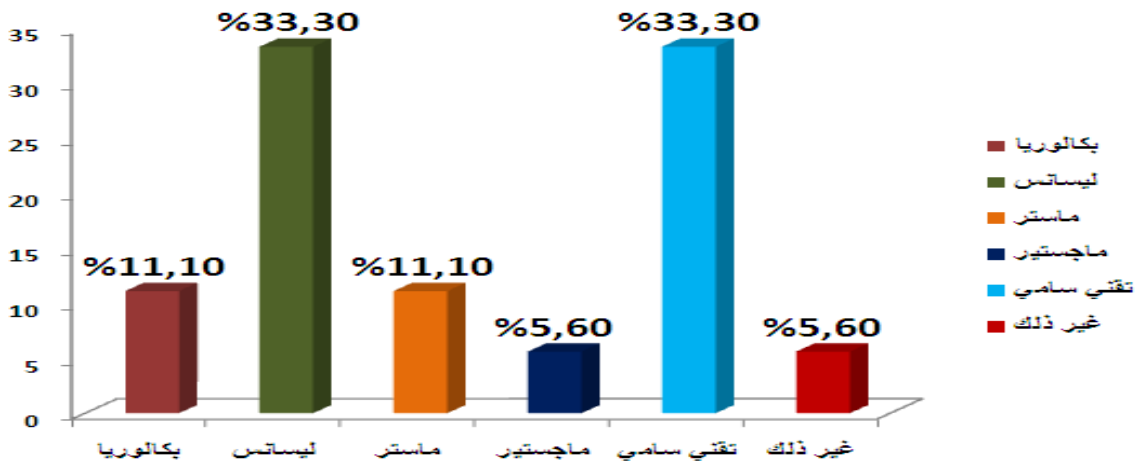
الشكل (2-10): توزيع الأفراد حسب المؤهل لمؤسسة اتصالات الجزائر



المصدر: من إعداد الطالب بناء على برنامج Spss

03-مؤسسة ليند غاز:

الشكل (2-11): توزيع حسب المؤهل العلمي لمؤسسة ليند غاز



المصدر: من إعداد الطالب بناء على برنامج Spss

يتضح من خلال مما سبق أن ما نسبته 55 الى 66 في المائة من عينة الدراسة، هم حاصلين على شهادة جامعية ليسانس وتقني سامي في جميع المؤسسات ، ونسبة لا تقل 11 في المائة حاصلين على شهادة الماستر، مما يعني أن حوالي 90 في المائة من أفراد عينة الدراسة هم حاصلين على شهادات جامعية، إذ يعد هذا مؤشرا هاما على أن أفراد العينة في مجملهم لديهم القدرة على الإجابة على أسئلة الاستبيان، وهذا من شأنه أن يعزز الثقة في الإجابات ويرفع من درجة الاعتماد عليه في التحليل .

رابعا: توزيع أفراد حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة :

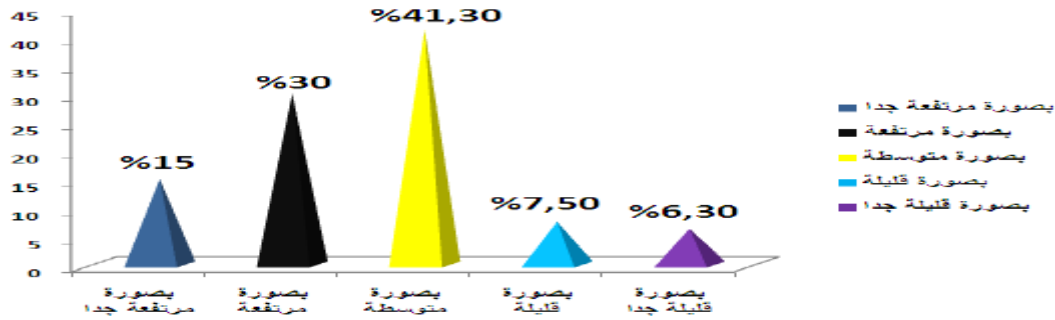
الجدول (2-15): توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة

ليند غاز		اتصالات الجزائر		سونلغاز		البيان
النسبة %	التكرار	النسبة %	التكرار	النسبة %	التكرار	
15,8	6	15,8	19	15,0	12	بصورة مرتفعة جدا
39,2	9	39,2	47	30,0	24	بصورة مرتفعة
28,3	2	28,3	34	41,3	33	بصورة متوسطة
13,3	1	13,3	16	7,5	6	بصورة قليلة
3,3	0	3,3	4	6,3	5	بصورة قليلة جدا

المصدر: من إعداد الطالب بناء على برنامج Spss

01- مؤسسة سونلغاز:

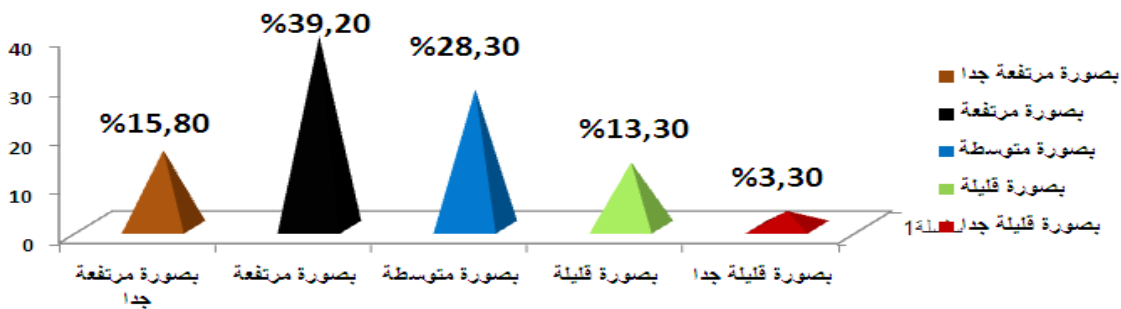
الشكل (2-12): توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة لمؤسسة سونلغاز



المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة اتصالات الجزائر:

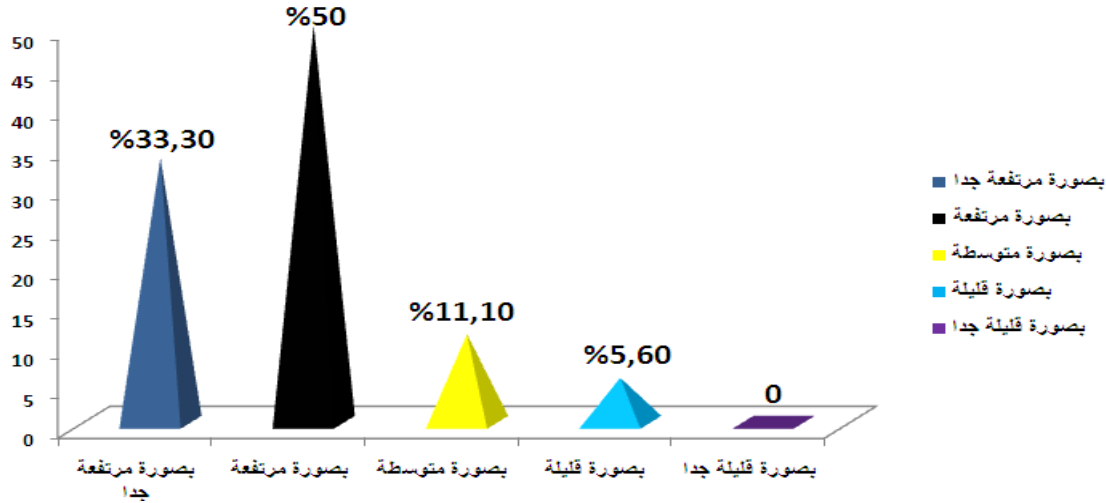
الشكل (2-13): توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة لمؤسسة اتصالات الجزائر



المصدر: من إعداد الطالب بناء على برنامج Spss

03- مؤسسة ليند غاز :

الشكل (2-14) : توزيع حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة لمؤسسة ليند غاز



المصدر: من إعداد الطالب بناء على برنامج Spss

يتضح من خلال أشكال السابقة حسب مدى استخدام المؤسسة لنظم المعلومات المحوسبة في المؤسسات محل الدراسة ، أن ما نسبته لا تقل عن 50 في المائة وكل مؤسسات تستخدم نظم المعلومات بين مرتفع إلى مرتفع جدا كما لوحظ نسبة 41 في المائة اتفقوا على متوسط بالنسبة مؤسسة سونلغاز .

خامسا :توزيع أفراد حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات :

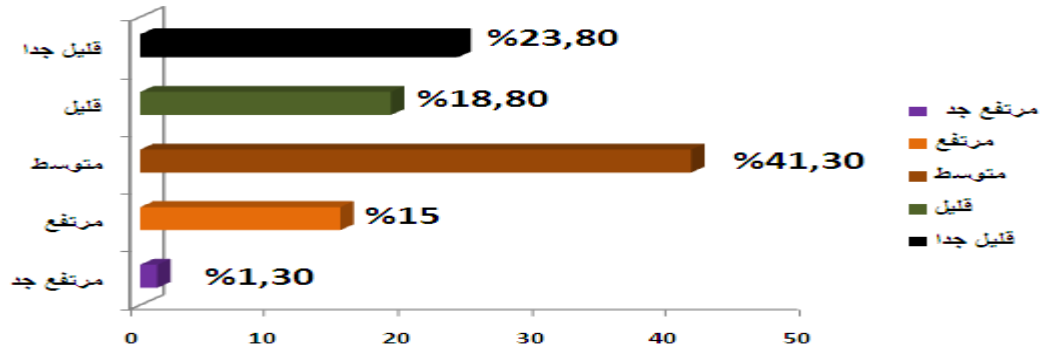
الجدول (2-16): توزيع حسب مستوى التدريب الذي يتلقونه مجال امن المعلومات

ليند غاز		اتصالات الجزائر		سونلغاز		البيان
النسبة %	التكرار	النسبة %	التكرار	النسبة %	التكرار	
16,7	3	5,0	6	1,3	1	مرتفع جدا
33,3	6	26,7	32	15,0	12	مرتفع
16,7	3	35,0	42	41,3	33	متوسط
22,2	4	19,2	23	18,8	15	قليل
11,1	2	14,2	17	23,8	19	قليل جدا

المصدر: من إعداد الطالب بناء على برنامج Spss

01- مؤسسة سونلغاز:

الشكل (2-15): توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات لمؤسسة سونلغاز

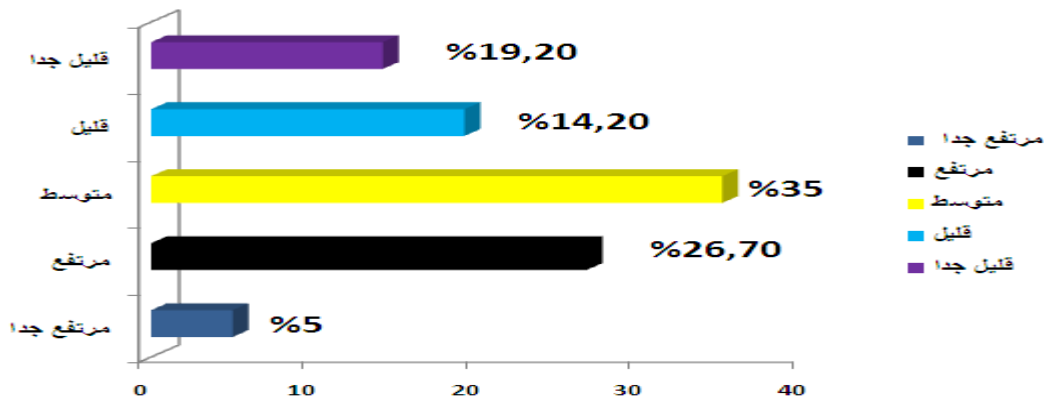


المصدر: من إعداد الطالب بناء على برنامج Spss

02- مؤسسة اتصالات الجزائر:

الشكل (2-16): توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات لمؤسسة

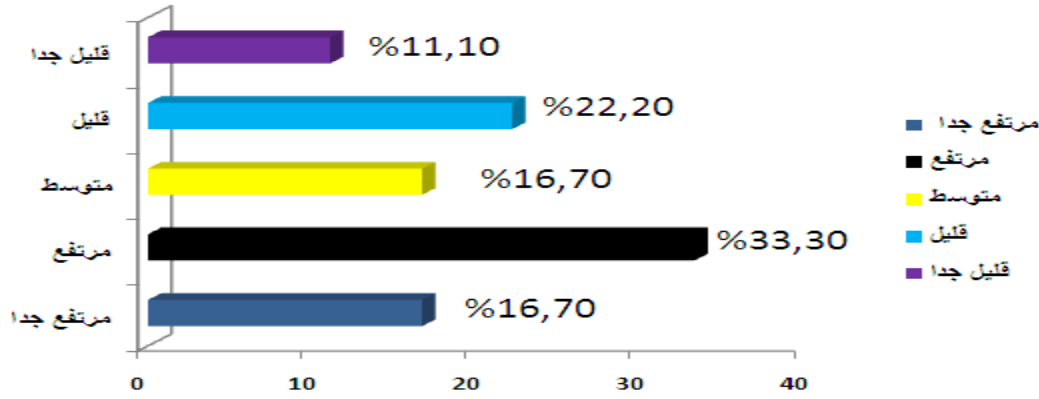
اتصالات الجزائر



المصدر: من إعداد الطالب بناء على برنامج Spss

03- مؤسسة ليندغاز:

الشكل (2-17): توزيع حسب مستوى التدريب الذي يتلقونه في مجال امن المعلومات لمؤسسة ليند غاز



المصدر: من إعداد الطالب بناء على برنامج Spss

يتضح من خلال ما سبق وحسب توزيع مستوى التدريب الذي يتلقونه في مجال امن المعلومات لوحظ إن المستوى تكوين متوسط إلى قليل التي سجل ما نسبته 41 في المائة في مؤسسة سونلغاز ولا تقل بكثير في مؤسستين ، وسجلت تكوين مرتفع نسبة 3,33 في المائة في ليند غاز وهذا يرجع إلى توجه الحديث في تكوين أمن نظم المعلومات وأهميته .

الفرع الثالث: قياس اتجاه أفراد العينة نحو عبارات الاستبيان

لوصول لنتائج الدراسة سنحاول في هذه المرحلة، وصف وتحليل إجابات عينة الدراسة، بخصوص تقييم ما مساهمة الأمن الكتروني من الحد من المخاطر نظم المعلومات ، ثم استنتاج اتجاه العينة لكل سؤال من أسئلة الدراسة، بناء على الأوزان المرجحة لمقياس ليكارت الثلاثي، على النحو التالي:

أولا: قياس اتجاه أفراد العينة نحو عبارات المحور الثاني :

الجدول (2-17): قياس اتجاه أراء أفراد العينة نحو المحور الثاني مخاطر نظم المعلومات

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

ليند غاز						اتصالات الجزائر						سونلغاز						المقياس	
الاتجاه	الانحراف المعياري	المتوسط المرجح	يحدث دائما	أحيانا	لم يحدث أبدا	الاتجاه	الانحراف المعياري	المتوسط المرجح	يحدث دائما	أحيانا	لم يحدث أبدا	الاتجاه	الانحراف المعياري	المتوسط المرجح	يحدث دائما	أحيانا	لم يحدث أبدا		
أحيانا	0,461	2,28	5	13	0	أحيانا	0,430	1,91	6	97	17	أحيانا	0,560	1,88	8	54	18	التكرار	سؤال 01
			27,8	72,2	0				5,0	80,8	14,2				10,0	67,5	22,5	النسبة	
لم يحدث أبدا	0,594	1,33	1	4	13	لم يحدث أبدا	0,605	1,64	8	61	51	لم يحدث أبدا	0,551	1,50	2	36	42	التكرار	سؤال 02
			5,6	22,2	72,2				6,7	50,8	42,5				2,5	45,0	52,5	النسبة	
أحيانا	0,639	1,94	3	11	4	أحيانا	0,612	1,75	11	68	41	أحيانا	0,560	1,70	4	48	28	التكرار	سؤال 03
			16,7	61,1	22,2				9,2	56,7	34,2				5,0	60,0	35,0	النسبة	
لم يحدث أبدا	0,857	1,50	4	1	13	أحيانا	0,690	1,61	14	45	61	لم يحدث أبدا	0,591	1,42	4	26	50	التكرار	سؤال 04
			22,2	5,6	72,2				11,7	37,5	50,8				5,0	32,5	62,5	النسبة	
لم يحدث أبدا	0,616	1,44	1	6	11	لم يحدث أبدا	0,657	1,65	12	54	54	أحيانا	0,601	1,64	5	41	34	التكرار	سؤال 05
			5,6	33,3	61,1				10,0	45,0	45,0				6,3	51,2	42,5	النسبة	
لم يحدث أبدا	0,236	1,06	0	1	17	لم يحدث أبدا	0,756	1,52	19	25	76	لم يحدث أبدا	0,599	1,29	6	11	63	التكرار	سؤال 06
			0	5,6	94,4				15,8	20,8	63,3				7,5	13,8	78,8	النسبة	
أحيانا	0,383	2,17	0	6	12	أحيانا	0,541	2,04	20	85	15	أحيانا	0,597	2,34	33	42	5	التكرار	سؤال 07
			0	33,3	66,7				16,7	70,8	12,5				41,3	52,5	6,3	النسبة	

التعليق:

أولا -مؤسسة سونلغاز:

01-التعليق على المحور الثاني المخاطر نظم المعلومات:

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-17) وبرجوع إلى (الملحق 02): قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثاني مخاطر نظم المعلومات الخاص بمؤسسة سونلغاز تبين أن الإجابات كانت في اتجاه "لم يحدث أبدا"، "أحيانا" بشكل متوسط، حيث لم يحظ أي سؤال بموافقة اتجاه العام الكلي لعينة و كما كان اتجاه العام لعبارة "يحدث دائما" وتحصل هذا المحور مخاطر نظم المعلومات على مجموع الكي لمتوسط الحسابي بالقيمة 1,59 بالانحراف المعياري مقدر 0,598 باتجاه العام "لم يحدث أبدا" وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة كمايلي:

1-1-اتجاه العام لأراء العينة نحو عبارة "لم يحدث أبدا "

كانت عبارة السادسة التي تنص " المرور غير الشرعي(غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أكثر العبارات "لم يحدث أبدا" من طرف العينة، إذا سجل 87,8 بالمائة ومتوسط المرجح 1,29 وكان الانحراف المعياري 0,599 يبرهن ان العينة كانت في هذا السؤال متوسطة التشتت يتفقون على إن المؤسسة لا يوجد المرور غير شرعي للبيانات أو النظام من خارج المؤسسة .
و كانت عبارة السابعة التي تنص " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات." أقل العبارات "لم يحدث أبدا" من طرف العينة، إذا سجل 06,3 بالمائة وهذا دليل على ان المؤسسة وإفرادها يتفقون ويصرحون إن الأجهزة تتعرض دائما إلى الفيروسات.

1-2- اتجاه العام لأراء العينة نحو عبارة "أحيانا"

كانت عبارة الأولى التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "أحيانا" من طرف العينة، إذا سجل 67,5 بالمائة ومتوسط المرجح 1,88 وكان الانحراف المعياري 0,560 ويتفقون على ان المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه
كانت عبارة السادسة التي تنص " المرور غير الشرعي(غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أقل العبارات "أحيانا" من طرف العينة، إذا سجل 13,8 بالمائة يبرهن ان العينة كانت في هذا السؤال متوسطة التشتت يتفقون على إن المؤسسة لا يوجد المرور غير شرعي للبيانات أو النظام من خارج المؤسسة .

1-3- اتجاه العام لأراء العينة نحو عبارة " يحدث دائما "

✚ و كانت عبارة السابعة التي تنص " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات. " أكثر العبارات " يحدث دائما " من طرف العينة، إذا سجل نسبة 41,3 بالمائة وهذا دليل على إن المؤسسة وإفرادها يتفقون ويصرحون إن الأجهزة تتعرض دائما إلى الفيروسات وهذا من شأنه يرفع من حدوث مخاطر نظم المعلومات .

✚ كانت عبارة الثانية التي تنص " الإدخال غير المتعمد (المقصود) للبيانات غير سليمة بواسطة الموظفين. " أقل العبارات " أحيانا " من طرف العينة، إذا سجل 02,5 بالمائة ويتفقون على ان المؤسسة لاتعاني من الإدخال المتعمد (المقصود) للبيانات غير سليمة بواسطة الموظفين هذا الأمر يعطي ثقة في المؤسسة إن الأفراد يحرصون على عدم تسريح بمعلومات زائفة وغير صحيحة

ثانيا: مؤسسة اتصالات الجزائر:

01- التعليق على المحور الثاني المخاطر نظم المعلومات:

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-17) ويرجع إلى (الملحق 02): قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثاني " مخاطر نظم المعلومات " الخاص بمؤسسة اتصالات الجزائر تبين أن الإجابات كانت في اتجاه " لم يحدث أبدا " ، " أحيانا " بشكل متوسط، حيث لم يحظ أي سؤال بموافقة اتجاه العام الكلي لعينة و كما كان اتجاه العام لعبارة " يحدث دائما " وتحصل هذا المحور "مخاطر نظم المعلومات "على مجموع الكي لمتوسط الحسابي بالقيمة 1,67 بالانحراف معياري مقدر 0,645 باتجاه العام "أحيانا" وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة اتصالات الجزائر كمايلي:

1-1- اتجاه العام لأراء العينة نحو عبارة "لم يحدث أبدا "

✚ كانت عبارة العشرة التي تنص " سرقة البيانات / المعلومات. " أكثر العبارات " لم يحدث أبدا " من طرف العينة، إذا سجل نسبة 65,8 بالمائة ومتوسط المرجح 1,42 وكان الانحراف المعياري 0,644 يبرهن إن العينة كانت في هذا السؤال متوسطة التشتت يتفقون على إن المؤسسة لا تتعرض لسرقة البيانات والمعلومات لا من داخل أو خارج المؤسسة .

✚ كانت عبارة السابعة التي تنص " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات. " أقل العبارات " لم يحدث أبدا " من طرف العينة، إذا سجل نسبة 12,6 بالمائة وهذا دليل على إن المؤسسة وإفرادها يتفقون ويصرحون إن الأجهزة تتعرض أحيانا إلى الفيروسات.

1-2- اتجاه العام لأراء العينة نحو عبارة "أحيانا"

✚ عبارة الأولى التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "أحيانا" من طرف العينة، إذا سجل نسبة 80,8 بالمائة ومتوسط المرجح 1,91 وكان الانحراف المعياري 0,430 ويتفوقون على إن المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه مثل مؤسسة سابقة .

✚ عبارة السادسة التي تنص " المرور غير الشرعي(غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أقل العبارات "أحيانا" من طرف العينة، إذا سجل نسبة 20,8 بالمائة يبرهن إن العينة كانت في هذا السؤال متوسطة التشتت يتفوقون على إن المؤسسة لا يوجد المرور غير شرعي للبيانات أو النظام من خارج المؤسسة .

1-3- اتجاه العام لأراء العينة نحو عبارة " يحدث دائما "

✚ وكان عبارة السابعة التي تنص " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات." أكثر العبارات " يحدث دائما" من طرف العينة، إذا سجل نسبة 16,7 بالمائة وهذا دليل على إن المؤسسة وإفرادها يتفوقون ويصرحون إن الأجهزة تتعرض دائما إلى الفيروسات وهذا من شأنه يرفع من حدوث مخاطر نظم المعلومات .

✚ عبارة الأولى التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أقل العبارات "يحدث دائما" من طرف العينة، إذا سجل نسبة 5 بالمائة ومتوسط المرجح 1,91 وكان الانحراف المعياري 0,430 ويتفوقون على إن المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين نسبة مبشرة بان حدوث دائما لهذا الأمر لانه صعب اكتشاف والقضاء عليه .

ثالثا- مؤسسة ليند غاز:

01-التعليق على المحور الثاني المخاطر نظم المعلومات:

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-17) وبرجوع إلى (الملحق 02) قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثاني " مخاطر نظم المعلومات" الخاص بمؤسسة ليند غاز تبين أن الإجابات كانت في اتجاه "لم يحدث أبدا" ، "أحيانا" بشكل متوسط، حيث لم يحظ أي سؤال بموافقة اتجاه العام الكلي لعينة و كما كان اتجاه العام لعبارة "يحدث دائما" قليلة جدا في معظم الاجابة وتحصل هذا المحور "مخاطر نظم المعلومات" على مجموع الكي لمتوسط الحسابي بالقيمة

1,47 بالانحراف معياري مقدر 0,478 باتجاه العام "لم يحدث أبدا" وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة ليند غاز كمايلي:

1-1- اتجاه العام لأراء العينة نحو عبارة "لم يحدث أبدا "

✚ كانت عبارة السادسة التي تنص " المرور غير الشرعي(غير المرخص به)للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أكثر العبارات " لم يحدث أبدا " من طرف العينة، إذا سجل 94,4 بالمائة ثم تاليه سؤل العشرة التي تنص " سرقة البيانات / المعلومات." الذي سجل نسبة 88,9 وهذا الدليل على إن المؤسسة يصعب المرور والسرقة البيانات

✚ عبارة الأول التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أقل العبارات "لم يحدث أبدا " من طرف العينة، إذا سجل نسبة 0 بالمائة تصريح واضح من العينة من إن ما ينص السؤل ممكن أن يقع أحيانا وغير متعمد

1-2- اتجاه العام لأراء العينة نحو عبارة "أحيانا"

✚ عبارة الأول التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "أحيانا " من طرف العينة، إذا سجل ما نسبته 72,2 بالمائة ويتفقون على إن المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه ويقع أحيانا ويوجد السؤل رقم أربعة عشرة و ينص على "تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية" بالنسبة 66,7 وتم السؤل الثالث و ينص "التدمير غير المتعمد(الحذف) للبيانات بواسطة الموظفين" بالنسبة 61,1.

✚ عبارة الرابع التي تنص " التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين " والسؤل السادس "المرور غير الشرعي(غير المرخص به)للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أقل العبارات "أحيانا " من طرف العينة، إذا سجل نسبة 5,6 بالمائة تصريح واضح من العينة أقل وقوع ولم يحدث أبدا .

1-3- اتجاه العام لأراء العينة نحو عبارة " يحدث دائما "

✚ عبارة الأول التي تنص " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "أحيانا " من طرف العينة، إذا سجل ما نسبته 27,2 بالمائة ويتفقون على إن المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه ويقع أحيانا

✚ وكانت عبارة السادسة إلى غاية آخر عبارة في الاستبيان اتفق كل المستجوبين أن " يحدث دائما " أقل النسبة 0 بالمائة وهذا يفسر أن المؤسسة لا تواجه إي نوع من المخاطر التي تم ذكرها في الاستبيان.

الجدول (2-18): قياس اتجاه آراء أفراد العينة نحو المحور الثالث نظام الأمن الالكتروني

البعد الأول : السياسات والإجراءات.

الاتجاه	ليند غاز					اتصالات الجزائر					سونلغاز					المقياس	سؤال		
	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح			موافق	محايد
محايد	0,832	2,11	7	6	5	محايد	0,728	2,26	51	49	20	موافق	0,779	2,34	42	23	15	التكرار	01
			38,9	33,3	27,8				42,5	40,8	16,7				52,5	28,7	18,8	النسبة	
موافق	0,575	2,72	14	13	1	موافق	0,597	2,62	81	32	7	موافق	0,638	2,65	59	14	7	التكرار	02
			77,8	16,7	5,6				67,5	26,7	5,8				73,8	17,5	8,8	النسبة	
موافق	0,616	2,56	11	6	1	موافق	0,692	2,34	56	49	15	موافق	0,738	2,39	43	25	12	التكرار	03
			61,1	33,3	5,6				46,7	40,8	12,5				53,8	31,3	15	النسبة	
موافق	0,594	2,67	13	4	1	موافق	0,661	2,51	72	37	11	موافق	0,763	2,49	52	15	13	التكرار	04
			72,2	22,2	5,6				60	30,8	9,2				65	18,8	16,3	النسبة	
موافق	0,514	2,83	16	1	1	موافق	0,645	2,57	78	32	10	موافق	0,763	2,49	52	15	13	التكرار	05
			88,9	5,6	5,6				65	26,7	8,3				65	18,8	16,3	النسبة	

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

سؤال 06	التكرار	11	17	52	2,51	0,729	موافق	21	49	50	2,24	0,733	محايد	4	4	10	2,33	0,840	محايد
	النسبة	13,8	21,3	65				17,5	40,8	41,7				22,2	22,2	55,6			
سؤال 07	التكرار	14	13	53	2,49	0,779	موافق	24	54	42	2,15	0,729	محايد	3	4	11	2,39	0,850	موافق
	النسبة	17,5	16,3	66,3				20	45	35				22,2	16,7	61,1			
سؤال 08	التكرار	32	20	28	1,95	0,870	محايد	17	60	43	2,22	0,676	محايد	7	3	8	2,28	0,752	محايد
	النسبة	40	25	35				14,2	50	35,8				16,7	38,9	44,4			
سؤال 09	التكرار	27	29	24	1,96	0,803	محايد	28	44	48	2,17	0,781	محايد	5	5	8	2,17	0,857	محايد
	النسبة	33,8	36,6	30				23,3	36,7	40				27,8	27,8	44,4			
سؤال 10	التكرار	14	26	40	2,32	0,759	محايد	12	43	65	2,44	0,671	موافق	1	2	15	2,72	0,669	موافق
	النسبة	17,5	32,5	50				10	35,8	54,2				5,6	11,1	83,3			
سؤال 11	التكرار	14	8	58	2,55	0,778	موافق	12	28	80	2,57	0,670	موافق	0	0	18	3	0,000	موافق
	النسبة	17,5	10	72,5				10	23,3	66,7				0	0	100			
مجموع البعد الأول : السياسات والإجراءات مؤسسة سونلغاز																			
مجموع البعد الأول : السياسات والإجراءات مؤسسة اتصالات الجزائر																			
مجموع البعد الأول : السياسات والإجراءات مؤسسة ليند غاز																			

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

البعد الثاني : إجراءات امن المعلومات المتعلقة بالعاملين .

ليند غاز						اتصالات الجزائر						سونلغاز						المقياس	
الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق		
محايد	0,826	2,28	9	5	4	موافق	0,699	2,38	60	45	15	محايد	0,836	2,10	32	24	24	التكرار	سؤال 12
			50	27,8	22,2				50	37,5	12,5				40	30	30	النسبة	
محايد	0,832	2,11	7	6	5	محايد	0,700	2,33	55	49	16	محايد	0,803	2,01	26	29	25	التكرار	سؤال 13
			38,9	33,3	27,8				45,8	40,8	13,3				32,5	36,3	31,3	النسبة	
محايد	0,808	2,22	8	6	4	محايد	0,698	2,32	54	50	16	محايد	0,787	2,01	25	31	24	التكرار	سؤال 14
			44,4	33,3	22,2				45	41,7	13,3				31,3	38,8	30	النسبة	
موافق	0,784	2,56	13	2	3	موافق	0,683	2,36	57	49	14	محايد	0,791	2,26	38	25	17	التكرار	سؤال 15
			72,2	11,1	16,7				47,5	40,8	11,7				47,5	31,3	21,3	النسبة	
محايد	0,808	2,22	8	6	4	محايد	0,710	2,24	48	53	19	محايد	0,752	2,06	25	35	20	التكرار	سؤال 16
			44,4	33,3	22,2				40	44,2	15,8				31,3	43,8	25	النسبة	

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

موافق	0,686	2,67	14	2	2	موافق	0,673	2,52	75	33	12	محايد	0,783	2,29	39	25	16	التكرار	سؤال 17
			77,8	11,1	11,1				62,5	27,5	10				48,8	31,3	20		
موافق	0,514	2,83	16	1	1	موافق	0,635	2,53	72	39	9	موافق	0,729	2,48	49	20	11	التكرار	سؤال 18
			88,9	5,6	5,6				60	32,5	7,5				61,3	25	13,8		
موافق	0,751	2,41	البعد الثاني : إجراءات امن المعلومات المتعلقة بالعاملين مؤسسة ليند غاز			موافق	0,685	2,38	البعد الثاني : إجراءات امن المعلومات المتعلقة بالعاملين مؤسسة اتصالات الجزائر			محايد	0,783	2,17	البعد الثاني : إجراءات امن المعلومات المتعلقة بالعاملين مؤسسة سونلغاز				

البعد الثالث : إجراءات امن المعلومات المتعلقة بالعتاد والبيانات

ليند غاز						اتصالات الجزائر						سونلغاز						المقياس	سؤال
الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق	الاتجاه	الانحراف المعياري	المتوسط المرجح	موافق	محايد	غير موافق		
موافق	0,767	2,67	15	0	3	موافق	0,682	2,43	64	43	13	محايد	0,808	2,33	43	20	17	التكرار	19
			83,3	0	16,7				53,3	35,8	10,8				53,8	25	21,3	النسبة	
موافق	0,236	2,94	17	1	0	موافق	0,607	2,63	84	28	8	محايد	0,874	1,91	27	19	34	التكرار	20
			94,4	5,6	0				70	23,3	6,7				33,8	23,8	42,5	النسبة	
موافق	0,669	2,72	15	1	2	موافق	0,635	2,52	72	39	9	موافق	0,789	2,40	47	18	15	التكرار	21
			83,3	5,6	11,1				60	32,5	7,5				58,8	22,5	18,8	النسبة	
موافق	0,594	2,67	13	4	1	موافق	0,620	2,55	74	38	8	محايد	0,776	2,33	41	24	15	التكرار	22
			72,2	22,2	5,6				61,7	31,7	6,7				51,2	30	18,8	النسبة	

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

موافق	0,705	2,56	12	4	2	موافق	0,620	2,42	63	45	12	موافق	0,758	2,41	46	21	13	التكرار	سؤال 23
			66,7	22,2	11,1				52,5	37,5	10				57,5	26,3	16,3	النسبة	
موافق	0,428	2,78	14	4	0	موافق	0,669	2,42	60	50	10	موافق	0,765	2,35	42	24	14	التكرار	سؤال 24
			77,8	22,2	0				50	41,7	8,3				52,5	30	17,5	النسبة	
موافق	0,698	2,61	13	3	2	موافق	0,658	2,43	63	46	11	موافق	0,759	2,42	47	20	13	التكرار	سؤال 25
			72,2	16,7	11,1				52,5	38,3	9,2				58,8	25	16,3	النسبة	
موافق	0,594	2,67	13	4	1	موافق	0,622	2,48	66	46	8	محايد	0,834	2,25	40	20	20	التكرار	سؤال 26
			72,2	22,2	5,6				55	38,3	6,7				50	25	25	النسبة	
موافق	0,616	2,56	11	6	1	موافق	0,677	2,39	60	47	13	موافق	0,792	2,43	46	16	15	التكرار	سؤال 27
			61,1	33,3	5,6				50	39,2	10,8				61,3	20	18,8	النسبة	

الجدول (2-19):مجموع الاتجاه الآراء الأفراد العينة الدراسة لمحور الثالث

ليند غاز			اتصالات الجزائر			سونلغاز			الأبعاد
الاتجاه	الانحراف المعياري	المتوسط المرجح	الاتجاه	الانحراف المعياري	المتوسط المرجح	الاتجاه	الانحراف المعياري	المتوسط المرجح	
لم يحدث أبدا	0,478	1,47	أحيانا	0,645	1,67	لم يحدث أبدا	0,598	1,59	المحور الثاني : مخاطر نظم المعلومات
موافق	0,645	2,52	موافق	0,689	2,37	موافق	0,763	2,37	البعد الأول : السياسات والإجراءات
مرافق	0,751	2,41	موافق	0,685	2,38	محايد	0,783	2,17	البعد الثاني : إجراءات امن المعلومات المتعلقة بالعاملين
موافق	0,600	2,67	موافق	0,647	2,47	محايد	0,798	2,30	البعد الثالث: إجراءات امن المعلومات المتعلقة بالعتاد و القاعدة البيانات
موافق	0,665	2,53	موافق	0,674	2,41	محايد	0,781	2,28	المحور الثالث: نظام الأمن الكتروني في المؤسسة

المصدر: من إعداد الطالب بناء على النتائج الاستبيان

التعليق:

أولا -مؤسسة سونلغاز:

02-التعليق على المحور الثالث نظام الأمن الكتروني :

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-18) ويرجع إلى (الملحق 02): قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثالث النظام الأمن الكتروني الخاص بمؤسسة سونلغاز تبين أن الإجابات كانت في اتجاه "غير الموافق"، "محايد"، "موافق" بشكل متوسط، حيث لم يحظ أي سؤال بموافقة اتجاه العام الكلي لعينة و تحصل هذا المحور "نظام الأمن الكتروني" على مجموع الكي لمتوسط الحسابي بالقيمة 2,28 بالانحراف معياري مقدر 0,781 باتجاه العام "محايد" ونلاحظ من النتائج ان المتوسط الحسابي يميل إلى اتجاه الموافق ونلاحظ إن الانحراف معياري يدل على وجود تشتت في الإجابات عكس المحور السابق وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة كمايلي:

1-2- اتجاه العام لأراء العينة نحو عبارة "غير الموافق "

نجد عبارة تحتل الرتبة الأولى في اتفاق و اعلي نسبة في البعد الأول "السياسات والإجراءات" محور " نظام الأمن الكتروني " السؤال الثامن الذي ينص على " يتم تجديد العتاد دوريا" حصل على اتفاق العينة بالنسبة 40 في المائة على عبارة "غير موافق" حصل على مجموع الكي متوسط الحسابي بالقيمة 1,95 بالانحراف معياري مقدر 0,870 وهذا دليل على إن المؤسسة تحتفظ بالعتاد لفترة يعتبرها الأفراد طويلة .

نجد عبارة تحتل الرتبة الأولى في اتفاق و اعلي نسبة في البعد الثاني " إجراءات امن المعلومات المتعلقة بالعاملين " محور " نظام الأمن الكتروني " السؤال الثالث عشر الذي ينص على " تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة " حصل على اتفاق العينة بالنسبة 31,3 في المائة على عبارة "غير موافق" حصل على مجموع الكي متوسط الحسابي بالقيمة 2,01 بالانحراف معياري مقدر 0,803 وهذا دليل على إن المؤسسة تحتفظ بالعتاد لفترة يعتبرها الأفراد طويلة .

ثم نجد عبارة اعلي نسبة في البعد الثالث " البعد الثالث : إجراءات امن المعلومات المتعلقة بالعتاد والبيانات " محور " نظام الأمن الكتروني " السؤال العشرون الذي ينص على " يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها." حصل على نسبة 42,5 في المائة بمتوسط المرجح 1,91 وانحراف معياري 0,789 وهذا دليل على عدم وجود البديل لطاقة وهذا تم إثباته في المقابلة مع رئيس المصلحة المعلوماتية .

2-2- اتجاه العام لأراء العينة نحو عبارة "محايد "

نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول "السياسات والإجراءات" محور " نظام الأمن الكتروني " السؤال التاسع الذي ينص على " يفرض على الموظفين تغيير كلمة المرور دوريا " حصل على اتفاق العينة بالنسبة 36,6 في المائة على عبارة "محايد" حصل على مجموع الكي متوسط الحسابي بالقيمة 1,96 بالانحراف معياري مقدر 0,803 وهذا دليل على إن المؤسسة لا تفرض على الموظفين تغيير كلمة المرور دوريا لان وجدنا الإجابات تنقسم بين المحايد والغير موافق

وتحصلت عبارة السادس عشر في البعد الثاني بنص "هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات" بالنسبة 43,8 لمتوسط الحسابي بالقيمة 2,06 بالانحراف معياري مقدر 0,752 يعني إن المؤسسة تضع السجل رقابي على حوادث الأمن المعلومات كما ثبت في المقابلة

كما تحصلت عبارة اثنان وعشرون بنص "كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها." على أكبر نسبة في البعد الثالث 30 في المائة حصل على مجموع الكي متوسط الحسابي بالقيمة 2,33 بالانحراف معياري مقدر 0,776 هذه النتيجة المتوسط تميل ميل كبير وتقسّم الإجابة مع الموافقة دليل قاطع إن المؤسسة لا تتعرض لمخطر العبث بكوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها

2-3- اتجاه العام لأراء العينة نحو عبارة "موافق "

✚ نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول "السياسات والإجراءات" لمحور " نظام الأمن الكتروني " السؤال الحادي عشر الذي ينص على " تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها " حصل على اتفاق العينة بالنسبة 72,5 في المائة على عبارة "موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,55 بالانحراف معياري مقدر 0,778 وكما هو في الملحق رقم 03 دليل على كتابة اسم الموظف في أي عملية

✚ وتحصلت عبارة الثامن عشر في البعد الثاني بنص " لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا " بالنسبة 61,3 لمتوسط الحسابي بالقيمة 2,48 بالانحراف معياري مقدر 0,729 يعني إن المؤسسة تخول صلاحيات لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا

✚ كما تحصلت عباراتي الواحد وعشرون و خمسة والعشرون و ينص على التوالي " يمنع الموظف الغير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات " و " توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن " على اكبر نسبة في البعد الثالث 58,8 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة على التوالي 2,40 و 2,42 بالانحراف معياري مقدر على التوالي 0,789 و 0,759 هذه نتيجتين جيدة لهذا البعد والذي شملت النسخ الإضافية و عدم إجراء تعديلات في مكونات المادية في نظم المعلومات ومن شأنه تقليل مخاطر المترتبة عنها .

ثانيا. -مؤسسة اتصالات الجزائر :

2-02-التعليق على المحور الثالث نظام الأمن الكتروني :

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-18) وبرجوع إلى (الملحق 02): قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثالث النظام الأمن الكتروني الخاص بمؤسسة اتصالات الجزائر تبين أن الإجابات كانت في اتجاه "غير الموافق" ، "محايد "موافق" بشكل متوسط، حيث لم يحظ أي سؤال بموافقة اتجاه العام الكلي لعينة و تحصل هذا المحور "نظام الأمن الكتروني" على مجموع الكي لمتوسط الحسابي بالقيمة 2,41 بالانحراف معياري مقدر 0,674 باتجاه العام "موافق " ونلاحظ إن الانحراف معياري يدل على وجود تشتت اقل في الإجابات المحور نفسه في سونلغاز وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة كمايلي:

2-1- اتجاه العام لأراء العينة نحو عبارة "غير الموافق "

✚ نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول "السياسات والإجراءات" لمحور " نظام الأمن الكتروني " عبارة التاسعة التي تنص على " يفرض على الموظفين تغيير كلمة المرور دوريا " حصل على اتفاق العينة بالنسبة 23,3 في المائة على عبارة "غير موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,17 بالانحراف معياري مقدر 0,781 إن المؤسسة لها دراية بأمن المعلومات على كلمة السر الموظفين إن تغيير دوريا وتفرض عليهم تغييرها دوريا وهذا بسبب نسبة أعلاه ضعيفة

نجد عبارة تحتل الرتبة الأولى في اتفاق و اعلي نسبة في البعد الثاني " إجراءات امن المعلومات المتعلقة بالعاملين " محور " نظام الأمن الكتروني " السؤال السادس عشر الذي ينص على " هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات " حصل على اتفاق العينة بالنسبة 15,8 في المائة على عبارة " غير موافق " حصل على مجموع الكي متوسط الحسابي بالقيمة 2,24 بالانحراف معياري مقدر 0,710 وهذا دليل على إن تضع السجل رقابي خاص بالأمن المعلومات والحوادث متعلقة به .

كما تحصلت عبارتي التاسع عشر و واحد والعشرون و ينص على التوالي " تستخدم المؤسسة شتى الوسائل (أبواب -أقفال - بطاقات دخول -كاميرات) لحماية مكونات نظم المعلومات " و " يتم تثبيت مضادات الفيروسات والتحديثات الدورية . " على أكبر نسبة في البعد الثالث 10,8 في المائة حصل على مجموع الكي متوسط الحسابي بالقيمة على التوالي 2,43 و 2,39 بالانحراف معياري مقدر على التوالي 0,682 و 0,677 هذه نتيجتين جيدة لهذا البعد والذي شملت عنصرين مهمين في الحد من المخاطر نظم المعلومات والتي تحمي العتاد ماديا و بتثبيت المضادات الفيروسات داخليا .

2-2- اتجاه العام لأراء العينة نحو عبارة " محايد "

نجد عبارات تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول " السياسات والإجراءات " محور " نظام الأمن الكتروني " السؤال الثامن الذي ينص على " يتم تجديد العتاد دوريا " حصل على اتفاق العينة بالنسبة 50 في المائة على عبارة " محايد " حصل على مجموع الكي متوسط الحسابي بالقيمة 2,22 بالانحراف معياري مقدر 0,676 وهذا دليل على إن المؤسسة تجدد العتاد دوريا هذا راجعا إلى مقدار المتوسط الذي يقترب إلى الموافق وتحصلت عبارة السادس عشر في البعد الثاني بنص " هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات " بالنسبة 41,7 في المائة بالمتوسط الحسابي بالقيمة 2,32 بالانحراف معياري مقدر 0,698 يعني إن المؤسسة تضع السجل رقابي على حوادث الأمن المعلومات كما ثبت في المقابلة.

وتحصلت عبارة الرابع والعشرون في البعد الثالث بنص " توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن. " بالنسبة 41,7 في المائة بالمتوسط الحسابي بالقيمة 2,42 بالانحراف معياري مقدر 0,669 .

2-3- اتجاه العام لأراء العينة نحو عبارة " موافق "

نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول " السياسات والإجراءات " محور " نظام الأمن الكتروني " السؤال الثاني الذي ينص على " تدرك الإدارة أهمية سياسات أمن المعلومات. " حصل على اتفاق العينة بالنسبة 67,5 في المائة على عبارة " موافق " حصل على مجموع الكي متوسط الحسابي بالقيمة 2,62 بالانحراف معياري مقدر 0,597 هذا الجواب جوهرى ومهم لان سياسات الأمنية لا تطبق إلا بدراية الإدارة العليا بأهمية نظم المعلومات

وتحصلت عبارة السابع عشر في البعد الثاني بنص " يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة. " بالنسبة 62,5 لمتوسط الحسابي بالقيمة 2,52 بالانحراف معياري مقدر 0,673 يعني إن المؤسسة تهتم بالأمن المعلومات وتدرك العواقب إذا احتلت ومنه تفرض العقوبات على من ينتهك ويتخالف الأوامر.

وتحصلت عبارة العشرون في البعد الثالث بنص " يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها " بالنسبة 70 في المائة بالمتوسط الحسابي بالقيمة 2,63 بالانحراف معياري مقدر 0,607 يعني إن المؤسسة لديها مولد كهرباء ومخزن الطاقة كما ثبت في المقابلة.

ثالثا. -مؤسسة ليند غاز:

02-التعليق على المحور الثالث نظام الأمن الكتروني :

بتحليل نتائج الاستبيان في الجدول أعلاه الجدول رقم (2-18) وبرجوع إلى (الملحق 02): قياس اتجاه أفراد العينة نحو عبارات الاستبيان متعلقة بمحور الثالث النظام الأمن الكتروني الخاص بمؤسسة ليند غاز تبين أن الإجابات كانت في اتجاه "غير الموافق"، "محايد" "موافق" بشكل متوسط، حيث حظي سؤال الحادي عشر بموافقة اتجاه العام الكلي لعينة و تحصل هذا المحور "نظام الأمن الكتروني" على مجموع الكي لمتوسط الحسابي بالقيمة 2,53 بالانحراف معياري مقدر 0,665 باتجاه العام "موافق" ونلاحظ إن الانحراف معياري يدل على وجود تشتت اقل في الإجابات المحور نفسه في مؤسستين سابقتين وكان تفصيل النتيجة المحور سالف الذكر الخاص بالمؤسسة كمايلي:

1-2-اتجاه العام لأراء العينة نحو عبارة "غير الموافق"

كما تحصلت عباراتي الأول و التاسع و ينص على التوالي " توجد في المؤسسة سياسات وإجراءات مكتوبة لأمن المعلومات " و " يفرض على الموظفين تغيير كلمة المرور دوريا." على أكبر نسبة في البعد الأول 27,8 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة على التوالي 2,11 و 2,17 بالانحراف معياري مقدر على التوالي 0,832 و 0,857. كما هو موضح في الجدول أعلاه.

نجد عبارة تحتل الرتبة الأولى في اتفاق و اعلي نسبة في البعد الثاني " إجراءات امن المعلومات المتعلقة بالعاملين " محور نظام الأمن الكتروني " السؤال الثالث عشر الذي ينص على " تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة " حصل على اتفاق العينة بالنسبة 27,8 في المائة على عبارة "غير موافق" حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,11 بالانحراف معياري مقدر 0,832 وهذا دليل على إن المؤسسة لها بعد نظر من الوصف والتوصيف الوظيفي تضع متطلبات ومعايير المنصب من البداية.

كما تحصلت عبارة التاسع عشر و ينص على " تستخدم المؤسسة شتى الوسائل (أبواب -أقفال - بطاقات دخول -كاميرات) لحماية مكونات نظم المعلومات " على أكبر نسبة في البعد الثالث 16,7 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة على 2,67 بالانحراف معياري مقدر ب 0,767 .

2-2-اتجاه العام لأراء العينة نحو عبارة "محايد"

نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول "السياسات والإجراءات" محور نظام الأمن الكتروني " السؤال الثاني الذي ينص على " تدرك الإدارة أهمية سياسات أمن المعلومات." حصل على اتفاق

العينة بالنسبة 16,7 في المائة على عبارة "محايد" حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,72 بالانحراف معياري مقدر 0,72 وهذا دليل على إن الإدارة تولي اهتمام ومؤشر المتوسط يثبت هذا تساوي نسبة عباراتي الثالث عشر ورابع عشر والسادس عشر في نسبة 33,3 والذي يحتوي على ما يلي على توالي " تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة " يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف ".
وتحصلت عبارة سبعة والعشرون في البعد الثالث بنص " يتم تثبيت مضادات الفيروسات والتحديثات الدورية. " بالنسبة 33,3 في المائة بالمتوسط الحسابي بالقيمة 2,56 بالانحراف معياري مقدر 0,616 .

2-3- اتجاه العام لآراء العينة نحو عبارة "موافق "

نجد عبارة تحتل الرتبة الأولى في اتفاق الأفراد العينة و اعلي نسبة في البعد الأول "السياسات والإجراءات" محور " نظام الأمن الكتروني " السؤال الحادي عشر الذي ينص على " تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها ". حصل على اتفاق العينة بالنسبة 100 في المائة على عبارة "موافق" حصل على مجموع الكي لمتوسط الحسابي بالقيمة 3 بالانحراف معياري مقدر 0,000 هذا الجواب معبر على اتفاق الكل وعدم وجود تشتت والمؤسسة تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها
وتحصلت عبارة الثامنة عشر في البعد الثاني بنص " لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا. " بالنسبة 88,9 لمتوسط الحسابي بالقيمة 2,83 بالانحراف معياري مقدر 0,514 يعني إن المؤسسة تهتم بكلمة السر الخاصة بالموظفين .
وتحصلت عبارة العشرون في البعد الثالث بنص " يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها " بالنسبة 94,4 في المائة بالمتوسط الحسابي بالقيمة 2,94 بالانحراف معياري مقدر 0,236 وتشير معطيات على عدم تشتت الإجابات يعني إن المؤسسة لديها مولد كهرباء ومخزن الطاقة كما ثبت في المقابلة أيضا.

الفرع الرابع : معامل سبيرمان للارتباط

الجدول (2-20): الارتباط سبيرمان للارتباط

معامل سبيرمان للارتباط.		سونلغاز		اتصالات الجزائر		ليند غاز	
		المحور الثالث : نظام الأمن الالكتروني في المؤسسة	المحور الثاني: مخاطر نظم المعلومات.	المحور الثالث : نظام الأمن الالكتروني في المؤسسة	المحور الثاني: مخاطر نظم المعلومات.	المحور الثالث : نظام الأمن الالكتروني في المؤسسة	المحور الثاني: مخاطر نظم المعلومات.
المحور الثالث : نظام الأمن الكتروني في المؤسسة	Correlation Coefficient Sig. (2-tailed) N	1,000 80	0,088 0,436 80	1,000 120	0,063 0,493 120	1,000 18	-0,550* 0,018 18
المحور الثاني: مخاطر نظم المعلومات.	Correlation Coefficient Sig. (2-tailed) N	0,088 0,436 80	1,000 80	0,063 0,493 120	1,000 120	-0,550* 0,018 18	1,000 18

*. Correlation is significant at the 0.05 level (2-tailed). ليند غاز

المصدر : من إعداد الطالب بناء على المخرجات SPSS v.20

التعليق:

من خلال جدول رقم(2-20) نجد النتائج الارتباط سبيرمان كالتالي :

➤ بالنسبة لمؤسسة سونلغاز : تحصلنا على القيمة الارتباط $R = 0.088$ عند $sig = 0.436$ وهي غير دالة إحصائيا إذ أنها يجب أن تكون اصغر من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة سونلغاز لا يساهم في الحد من المخاطر. و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.

➤ بالنسبة لمؤسسة اتصالات الجزائر : تحصلنا على القيمة الارتباط $R = 0.063$ عند $sig = 0.493$ وهي غير دالة إحصائيا إذ أنها يجب أن تكون اصغر من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة اتصالات الجزائر لا يساهم في الحد من المخاطر. و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.

➤ بالنسبة لمؤسسة ليند غاز : تحصلنا على القيمة الارتباط $R = -0.55$ عند $sig = 0.018$ وهي دالة إحصائيا إذ أنها اصغر من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة ليند غاز يساهم في الحد من المخاطر. و نستنتج انه توجد علاقة ارتباط عكسية قوية ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.

المطلب الثاني: المناقشة النتائج

الفرع الأول: المناقشة

أولا : مؤسسة سونلغاز: من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، يتضح أن المؤسسة تمتلك الجانب البشري في موقعين مختلفين، مكونات موجودة على مستوى موقع فرع ELIT بالجزائر العاصمة، المختص في إنجاز وتسيير وتطوير نظم المعلومات الإلكترونية المستخدمة في شركات مجمع سونلغاز وتمثل في كل من الموارد البشرية ؛ قواعد البيانات ؛ الأجهزة الإلكترونية ؛ شبكة الاتصالات ؛ السياسات الأمنية المعتمدة لحماية الأجهزة والمعلومات، ومكونات مت واجدة على مستوى كل مواقع ، ومن بينها مديرية التي أجرينها فيها دراسة الحالة، وتمثل في الم وارد البشرية ؛ الإجراءات المحاسبية ؛ المستندات والوثائق الثبوتية ؛ الأجهزة الإلكترونية ؛ شبكة الاتصالات ؛ السياسات الأمنية لحماية الأجهزة والمعلومات.

تحتوي نظم المعلومات المحاسبية الإلكترونية على مجموعة من المكونات والأجزاء التي يمكن أن تتواجد في مواقع مختلفة، مما يجعل هذه النظم عرضة للكثير من الأخطار والتهديدات، والتي قد تحدث عن قصد أو بغير قصد وتكون كما يلي: الوصول غير المرخص إلى قواعد البيانات ؛ عدم كفاءة إجراءات حماية قواعد البيانات

اكتشاف الآلية السرية لحماية النظام أو تعطيلها ؛ الأعطال في البرمجيات بسبب عرضي أو عن طريق تخريب للتجهيزات؛ تحصلنا على القيمة الارتباط غير دالة إحصائيا ، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة سونلغاز لا يساهم في الحد من المخاطر. و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.

ثانيا : اتصالات الجزائر : من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، يتضح أن المؤسسة تمتلك الجانب البشري فعال ولديها إطارات تكفي لإشراف نظام المعلومات بصفة كاملة والمؤسسة حاليا تحدث بعض التغييرات من اجل تحسين البرنامج قايما 05 إلى قايما 07 وانتقال عملية الإشراف على المستوى الخادم إلى الجزائر العاصمة كما اتضح لنا بالمقابلة بعض المميزات يتميز النظام بسرعة تنفيذ المهام و بسهولة مراقبة سيرورة العمل كما يساعد على اتخاذ القرار من خلال تزويد المسؤولين بكل المعلومات الضرورية وفي الوقت المناسب وايضا يعتبر وسيط بين أجهزة الاتصالات والموظفين بوصول سريع وآمن للأجهزة كما لا يخلو من نقائص والإخطار تحدد النظام منها لا توجد مذكرات مصلحيه تحت على الأمن أو إجراءاته، وهذه من أكبر العيوب و في حالة انقطاع الخدمة، تبقى التعليمات عالقة مما يستدعي تدخل نصف إلى للأوامر و نسخ البرامج في بعض حواسيب العمال ليست أصلية مما يعرض الحواسيب للتعطيل في حال تمت ترقية البرامج؛ شبكة X25 ثقيلة نوعا ما مقارنة بشبكة IP، مما يستدعي ترقيتها في حالة الطباعة يتم تحويل الملفات بواسطة فلاش ديسك مما يعرض المعلومات للضياع والفيروسات؛ كما من خلال تحليل الإجراءات الأمنية المطبقة على المكونات المادية لنظام المعلومات بما في ذلك الخوادم والملحقات وأجهزة الطاقة والتبريد وكذا مكان تواجد الأجهزة وكذلك تلك الإجراءات المطبقة على حماية البرامج ، من وجود نظام تشغيل UNIX، ومضادات الفيروسات والوصول بواسطة بروتوكول تلتنت ، كل هذه الإجراءات أكدت وحسب تصريح مدير هيئة ، لم يسجل أي توقف للخوادم وبالتالي الخدمة منذ أن تم فتح هذا المركز سنة 2004، وأن الإنقطاعات التي تحدث أحيانا على مستوى الوكالات التجارية سببها عادة خلل في الشبكة وليست الأجهزة ، مما سبق نستنتج أن للسياسات الأمنية دور كبير في ديمومة عمل نظام المعلومات.

ومن خلال نتائج تحصلنا على القيمة الارتباط غير دالة إحصائيا وإن نظام الأمن الالكتروني في مؤسسة اتصالات الجزائر لا يساهم في الحد من المخاطر. و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.

ثالثا : مؤسسة ليند غاز : من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، يتضح أن المؤسسة تمتلك الجانب البشري قليل ولكن يعتبر كافي لصغر الوحدة و ورقلة ولتطبيق الثقافة الاروبية يقلل الأفراد ويوسع في المهام والصلاحيات وكما وجدنا إن المؤسسة تملك العتاد والبرامج متطورة مثل ERP وسياج وتراكيت في تسيير وتتكون قاعدة البيانات المؤسسة لنظام المعلومات من خادم من نوع Microsoft بسعة صغيرة تقدر ب1.5 تيرا ولكن كافية لتخزين معلومات الوحدة وبدورها تنقل المعلومات لتخزينها على مستوى الجزائر العاصمة وهذا الخادم تم تقسيمه إلى خادم ثلاثي افتراضية -نقطة توزيع- نقطة طباعة - نقطة الثالثة وتحتوي على البرامج وتحديثات ومضادات الفيروسات المرخصة فقط من طرف الشركة لإلام ولكن لوحظ نقص في المستوى المؤسسة نقص الكاميرات المراقبة التي جاري توصيلها إلى المؤسسة وكما تبين ان المؤسسة لا تملك نظام الإطفاء الحرائق جيد هذا من شأنه يرفع تهديدات المحدقة بنظام المؤسسة ولكونها مؤسسة غازات الصناعية يكون الخطر مرتفعة في حد ذاته وكما اطلعنا على الوثائق المؤسسة تبين لنا إن المؤسسة حائزة على عدة شهادات جودة (ايزو) و تولي المؤسسة اهتمام بالأمن الالكتروني ولديها معرفة الجيدة ولكن توجد بعض النقائص والتي نراها خطر تحدد نظام منها استعانة الدائمة والمستمرة إلى عمال الاتصالات الجزائر في الشبكات والاتصالات واستعانة بالورشه تصليح الأجهزة الإعلام خارج المؤسسة ، ولكن من ملاحظة نتائج تحصلنا على القيمة الارتباط معبرة عن الدراسة ، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة ليند غاز يساهم في الحد من

الفصل الثاني: الدراسة الميدانية لتقييم اثر الأمن الالكتروني في الحد من المخاطر النظم المعلومات

المخاطر. و نستنتج انه توجد علاقة ارتباط عكسية قوية ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر و خلاصة القول واثبات صحة العلاقة بين السياسات الأمنية و المخاطر يعني كلما كانت الإجراءات الأمنية فعالة تنقص من احتمال حدوث المخاطر النظم المعلومات .

الفرع الثاني : المقارنة بين السياسات الأمنية عينة الدراسة

الجدول (2-21): المقارنة بين السياسات الأمنية المتبعة من المؤسسات عينة الدراسة

المؤسسة	سونلغاز	اتصالات الجزائر	ليند غاز
السياسات الأمنية			
مضادات الفيروسات	موجودة غير شاملة كل الأجهزة	موجودة غير شاملة كل الأجهزة	موجودة
عدم استعمال فلاش ديسك	غير مطبقة	غير مطبقة	مطبقة
كاميرات مراقبة	موجودة	موجودة	غير موجودة حاليا
تحديد الصلاحيات بدقة	مطبقة	مطبقة	مطبقة
كلمة السر شخصية لكل فرد	مطبقة	مطبقة	مطبقة
تغيير كلمة السر دوريا	مطبقة	مطبقة	مطبقة دوريا
الجدار الناري(العتاد)	موجود	موجود	موجود
مضادات الحرائق	موجودة	موجودة	غير موجودة
إنذارات السرقة	موجودة	غير موجودة	موجودة
إجراءات و سياسات أمنية مكتوبة	غير الموجودة	غير الموجودة	موجودة
الصيانة الدورية	موجودة	موجودة	موجودة
صيانة داخلية	داخليا	داخليا	داخليا وخارجية
دورات تحسيسية دورية في امن المعلومات	قليلة	متوسط	معتبرة
برامج حماية الشبكة	موجودة	موجودة	موجودة وفعالة
نسخ احتياطية	موجودة	موجودة	موجودة
نسخ احتياطية خارج المؤسسة	موجودة في ELIT	موجودة في المديرية	موجودة في المجمع
تشفير البيانات المهمة	مطبقة	مطبقة	مطبقة
مولد الكهرباء	غير موجود	موجود	موجود
مخزن ومعدل الكهرباء	موجود	موجود	موجود

المصدر: من إعداد الطالب بناء على النتائج المقابلة والملاحظة

الفرع الثالث : مدى إمكانية حدوث مخاطر نظام المعلومات:

في الجدول أسفله رقم (2-22) و بناء على الملاحظة والمقابلة نستخلص المخاطر ودرجة حدوثها في المؤسسات محل الدراسة كالآتي :

الجدول (2-22):المقارنة مدى إمكانية حدوث مخاطر نظام المعلومات بين المؤسسات عينة الدراسة

المخاطر	المؤسسة	سونلغاز	اتصالات الجزائر	ليند غاز
المتعلقة بالمدخلات	متوسط	متوسط	متوسط	منخفض
سرقة بيانات	منخفض	منخفض	متوسط	منخفض
انتحال شخصية	منخفض	منخفض	منخفض	منخفض
الفيروسات	مرتفع	مرتفع	مرتفع	منخفض
استعمال فلاش ديسك	مرتفع	مرتفع	مرتفع	متوسط
المخرجات زائفة	مرتفع	مرتفع	مرتفع	منخفض
مخطر اختراق الشبكة	منخفض	منخفض	منخفض	منخفض
مخطر الانترنت في المؤسسة	منخفض	منخفض	مرتفع	متوسط
مخطر انقطاع الكهرباء	مرتفع	مرتفع	منخفض	منخفض
عدم وجود أهداف ورؤية الإستراتيجية أمن نظام المعلومات	مرتفع	مرتفع	مرتفع	منخفض
عدم وجود الإجراءات الأمنية	منخفض	منخفض	مرتفع	منخفض
عدم وجود تدقيق في المجال الأمن نظام المعلومات	منخفض	منخفض	متوسط	منخفض
غياب البنية الشبكة	منخفض	منخفض	منخفض	منخفض
عدم توفير لوازم الأمنية لحفاظ على الخوادم ماديا	منخفض	منخفض	منخفض	مرتفع

المصدر :من إعداد الطالب بناء على النتائج المقابلة والملاحظة

خلاصة الفصل :

حاولنا في هذا الفصل إسقاط الدراسة النظرية على عينة الدراسة ، من خلال معرفة واقع نظامها المعلوماتي الإلكتروني، والسياسات الأمنية المتبعة وتحديد أثرها في الحد من المخاطر نظم المعلومات، بدءا باستعمال أداة المقابلة في تشخيص نظام المعلومات الإلكتروني لمؤسسات محل الدراسة ، وركزنا في ذلك على مكوناته و عناصره بالتفصيل، بالإضافة إلى الوقوف على الإجراءات والسياسات المعتمدة في الحفاظ على أمن النظام وسلامته، وبالمقابل استعملنا أداة الاستبيان لمعرفة مدى مساهمة الأمن الإلكتروني في الحد من المخاطر ، ومعرفة درجة هذا التأثير، ودلت نتائج هذه الدراسة على أن نظام المعلومات الإلكتروني، يستند إلى مجموعة مكونات تتألف من أفراد مؤهلين وبنية تحتية للأجهزة الإلكترونية والمعلوماتية، ساهمت في جعل النظام يرصد ويتصدى كل المخاطر وبالمقابل أظهرت الدراسة بعض العقبات التي تواجه النظام، وتحول دون تحقيقه لكامل تطلعات مستخدميه. أما في ما يتعلق بنتائج أداة الاستبيان فقد دلت على وجود تأثير لنظام المعلومات الإلكتروني في مؤسسات محل الدراسة .

و كانت أهم النتائج المتوصل إليها في هذا الفصل:

- ✓ توجد مجموعة من المخاطر التي تهدد نظام المعلومات؛
- ✓ يمكن السيطرة على هذه المخاطر من خلال فرض سياسات أمنية على مختلف المستويات؛
- ✓ إذا لم ترافق السياسات الأمنية منشورات وتعليمات تبين مخاطر نظم المعلومات و تحث على تطبيق السياسات الأمنية قد لا يستوعب الأفراد المخاطر المحيطة بنظم المعلومات.



الخاتمة



وكما باقي المنظمات والمؤسسات والشركات العالمية ، عمدت المؤسسات الجزائرية العاملة في مختلف القطاعات إلى استخدام تكنولوجيا المعلومات والاتصالات واستثمرت في بناء نظم وتطبيقات الحاسوب للقيام بعملياتها التشغيلية على صعيد الأعمال اليومية الروتينية والعمليات الإدارية المعقدة.

واتخاذ القرارات والعمل الإلكتروني ووفرت مستخدمي النظام إمكانات الاتصال بالانترنت للتواصل مع مشرفوهم و رؤسهم في حلقات الإدارية الإلكترونية المباشرة وغير المباشرة ، إمكانات مختلفة للوصول للمعلومات التي تناسبهم عبر الشبكات المحلية أو من خلال مواقع الويب العامة الوصول، وكان لهذا كله الأثر الكبير في ضرورة تفعيل أكبر لدور أمن المعلومات ليكون حاضرا أمام كل هذه التحديات المتجددة، وتسعى المؤسسات لتطوير نظم معلوماتها بقدراتها الذاتية أو من خلال الاستعانة بأطراف خارجية وتستند الشركات الكبرى على أنظمة معلومات قوية ، ومهيكله بطريقة جيدة ، لكي تتمكن من مواجهة كم المعلومات الهائل لعملائها ، حيث تلعب هذه الأنظمة دورا محوريا ، لاستمرارية نشاط هذه الشركات ، حيث كلما كان نظام المعلومات أكثر تكامل ، كلما كانت النتائج المرجوة أقرب إلى التحقيق داخل المنظمة أو الشركة ويبقى نظام المعلومات داخل مؤسسات الجزائرية دون التطلعات المرجوة ، بالرغم من كل الإيجابيات التي يحتويها، كون هذه المؤسسات محل الدراسة هي رائدة ومحتكرة في مجال التي تنشط فيه في الوطن ، فالأحرى وأفضل لهم إن تعكس هذه الريادة واحتكار داخل كياناتها .

أولا - نتائج اختبار الفرضيات:

تم اختبار الفرضيات في الدراسة الميدانية للإجابة على الإشكالية الرئيسية والمتمثلة بمدى مساهمة نظام الأمن الإلكتروني في الحد من المخاطر نظم المعلومات في شركات محل الدراسة ، وكانت النتائج كما يلي:

1- الفرضية الأولى : " تتميز نظم المعلومات في عينة الدراسة بالكفاءة من خلال المكونات (المادية و البرمجيات) ".

أولا: مؤسسة سونلغاز :

يتبين من خلال التحليل المتعلق بالفرضية الأولى بناء على استنتاجات المقابلة والدراسة الميدانية ، أن نظام المعلومات الإلكتروني في شركة سونلغاز، يتميز ببنية تحتية للأجهزة وتقنيات وبرمجيات إلكترونية ،و التي تتميز بالسرعة الفائقة في معالجة المعلومات واسترجاعها وقدرة التخزين الهائلة لقواعد البيانات، بالإضافة للمورد البشري المؤهل من مشرفون على التسيير النظام ومختصين في المعلوماتية واعتماد على ELIT الذين يقع على عاتقهم القيام بعمليات تحليل وتصميم وتسيير نظام المعلومات الإلكتروني ، مما أكسبه ميزة الاقتصاد في الجهد والوقت، مقارنة بالنظام اليدوي ،و لكن

بالمقابل وبناءا على نتائج المقابلة، يواجه نظام المعلومات بعض العقبات التي تحد من تحقيق كامل تطلعات مستخدميه ونظام المعلومات المثالي ومتكامل.

ثانيا : مؤسسة اتصالات الجزائر :

يتبين من خلال التحليل المتعلق بالفرضية الأولى بناءا على استنتاجات المقابلة والدراسة الميدانية على كفاءة المكونات المادية لنظام المعلومات والبرامج واتضح إن الخوادم والملحقات وأجهزة الطاقة والتبريد وكذا مكان تواجد الأجهزة وكذلك تلك الإجراءات المطبقة على حماية البرامج ، من وجود نظام تشغيل UNIX، ومضادات الفيروسات ومن تصريحات مدير هيئة لم يسجل أي توقف للخوادم منذ أن تم فتح هذا المركز سنة 2004 ولكن لم يمنع أن المؤسسة تحسن من البرامج وتطويرها ودليل ذلك انتقال من قايا 05 إلى قايا 07 أكثر تطورا و مع انتقال الخوادم إلى العاصمة ومركزية التخزين هذا من شأنه رفع درجة ادراك اهمية الامن المعلومات ومكوناته لمؤسسة .

ثالثا : مؤسسة ليند غاز :

من خلال ما تم ملاحظته، وجمعه خلال الدراسة الميدانية ، يتضح أن المؤسسة تمتلك الجانب البشري قليل ولكن يعتبر كافي لصغر الوحدة و وكما وجدنا إن المؤسسة تملك العتاد والبرامج متطورة مثل ERP وسياج وتراكيث في تسيير وتكون قاعدة البيانات المؤسسة لنظام المعلومات من خادم من نوع Microsoft بسعة صغيرة تقدر ب1.5 تيرا ولكن كافية لتخزين معلومات الوحدة وبدورها تنقل المعلومات لتخزينها على مستوى الجزائر العاصمة وهذا الخادم تم تقسيمه إلى خادم ثلاثي افتراضية -نقطة توزيع- نقطة طباعة -نقطة الثالثة و تحتوي على البرامج وتحديثات ومضادات الفيروسات المرخصة فقط من طرف الشركة لإلام ولكن لوحظ نقص في المستوى المؤسسة من جانب الحفاظ على مكونات النظم المعلومات نقص الكاميرات المراقبة وا لإطفاء الحرائق التي جاري توصيلها إلى المؤسسة ولكن لا يقلل من كفاءة نظام المعلومات المؤسسة وفعاليته من شتى الجوانب المادية والبرمجية .

✓ وبناءا عليه الفرضية الأولى محققة.

2-الفرضية الثانية : " لدى المؤسسات محل الدراسة نظام امن الكتروني يشمل كل عناصر الأمن الالكتروني لحماية أنظمتها من كل أنواع الاختراق "

أولا : مؤسسة سونلغاز :

بالرجوع إلى الدراسة الميدانية لسياسات الأمنية يتبين أن هناك إجراءات أمنية والإجراءات الاحترازية موضوعة من طرف المؤسسة لكل العناصر الأمن الكترونية من ناحية الشبكات و من ناحية العتاد و من ناحية الأفراد... الخ ، أن توافر سياسات أمنية عالية مطبقة على مستوى المكونات المادية والبرمجية لنظام المعلومات قد لا تكون كافية في حالة عدم تحسيس العنصر البشري بهذه السياسات ومشاركتهم فيها، وبالتالي وفي حالتنا هاته نجد أن الأفراد العاملون على نظم المعلومات لا يتمتعون بدرجة الوعي الكافي لتجنب مختلف الأنواع الاختراق ولكن المؤسسة تعتمد على مهندسو ELIT لهم دراية كافية لتصدي مختلف أنواع الاختراق البرمجي ولكن الاختراق المادي يقتصر على الأفراد نظام المعلومات

ثانيا : مؤسسة اتصالات الجزائر :

بالرجوع إلى الدراسة الحالة السياسات الأمنية المتبعة يتبين أن هناك إجراءات أمنية والإجراءات الاحترازية موضوعة من طرف المؤسسة لكل العناصر الأمن الكترونية من ناحية الشبكات و من ناحية العتاد و من ناحية الأفراد... الخ ، أن توافر سياسات أمنية عالية مطبقة على مستوى المكونات المادية والبرمجية لنظام المعلومات قد لا تكون كافية في المؤسسة لحماية نظام من الاختراق لوحظ في الدراسة إن مؤسسة اتصالات الجزائر رائدة في اتصالات ولكن تعاني من ناحية الشبكات وتعتمد على شبكة الويفي، التي يمكن أن تشكل ثغرة لاختراق النظام من خلال دخول أشخاص غرباء لشبكة المؤسسة التي صرح المدير المصلحة أنها تعرضت عديد من المرات إلى اختراق من خارج ومن داخل المؤسسة .

ثالثا : مؤسسة ليند غاز :

اتضح من دراسة ميدانية لنظام امن الكتروني مؤسسة وجد انه يشمل كل عناصر الأمن الالكتروني لحماية نظام من جميع نواحي السياسات خاصة بإفراد و الخاصة البرامج والعتاد... الخ ولكن من خلال ما وجد في المؤسسة إن نظام الحماية شبه مستحيل الاختراق لما رأيته من إحكام في الإجراءات الأمنية في دخول إلى مؤسسة عموما والى العتاد وبرامج خصوصا خصوصا كما ان المؤسسة على مستوى مجمع لها برنامج اسمه العنكبوت برنامج يخول لمسؤول دخول الى أي جهاز في مستوى الوحدات واذا ما لحظ وجود فيروس فقط يفتح تحقيق على مستوى وحدة لان من المستحيل مرور أي ناقل قابل للازالة في شبكة العتاد دون معرفة من قام بتوصيله

✓ وبناء عليه الفرضية الثانية محققة جزئيا

3-الفرضية الثالثة: "تحيط بأنظمة معلومات المؤسسات محل الدراسة العديد من المخاطر نلخصها في: مخاطر تتعلق

بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة"

أولا : مؤسسة سونلغاز :

من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، تبين أن هناك مخاطر تحيط بأنظمة معلومات المؤسسات محل الدراسة عموما مؤسسة سونلغاز خاصتا، حسب مراحل النظام مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة، لكن من خلال تحليل الاستبيان تبين أن العينة تعتقد بوجود مخاطر مترددة ، ومن المتوسط الحسابي للعينة الذين أقرؤا بوجود مخاطر متعلقة بنظام بمتوسط المرجح إدراك الأفراد حول مخاطر المحدقة بنظام المعلومات ، ويلاحظ ذلك كذلك حين الرجوع للسؤال الثاني في محور نظام الأمن الكتروني في المؤسسة الذي ينص "تدرك الإدارة أمية سياسات أمن المعلومات " فقد كانت إجابة العينة قوية بموافقة بمتوسط .

ثانيا : مؤسسة اتصالات الجزائر :

من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، تبين أن هناك مخاطر تحيط بأنظمة معلومات المؤسسات محل الدراسة عموما مؤسسة الاتصالات الجزائرية خاصتا، حسب مراحل النظام مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة، لكن من خلال تحليل الاستبيان تبين أن العينة تعتقد بوجود مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة غير مترددة، ومن خلال الجدول رقم (2-17) فقد كان المتوسط الحسابي للعينة الذين أقرؤا بوجود مخاطر متعلقة بنظام بمتوسط المرجح = 1.67 ، إدراك الأفراد حول مخاطر المحدقة بنظام المعلومات ، ويلاحظ ذلك كذلك حين الرجوع للسؤال الثاني في محور نظام الأمن الكتروني في المؤسسة الذي ينص "تدرك الإدارة أمية سياسات أمن المعلومات " فقد كانت إجابة العينة قوية بموافقة بمتوسط مقدرة 2,62، لكن نلاحظ عدم مقدرة المؤسسة على تجنب حدوث المخاطر عند دراسة نظام المعلومات.

ثالثا: مؤسسة ليند غاز :

من خلال ما تم ملاحظته، وجمعه خلال الدراسة الميدانية، تبين أن هناك مخاطر تحيط بأنظمة معلومات المؤسسات محل الدراسة عموما مؤسسة ليند غاز خاصتا، حسب مراحل النظام مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة، لكن من خلال تحليل الاستبيان تبين أن العينة تعتقد بوجود مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، مخاطر تتعلق بالبيئة بدرجة مترددة ، ومن خلال ما توصلنا له فقد كان المتوسط الحسابي للعينة الذين أقرؤا بوجود مخاطر متعلقة بنظام بمتوسط المرجح = 1.47 ، إدراك الأفراد حول مخاطر المحدقة بنظام المعلومات ، ويلاحظ ذلك كذلك حين الرجوع للسؤال الثاني في محور

نظام الأمن الإلكتروني في المؤسسة الذي ينص "تدرك الإدارة أهمية سياسات أمن المعلومات " فقد كانت إجابة العينة قوية بموافقة بمتوسط مقدرة 2,72، لكن نلاحظ مقدرة المؤسسة على تجنب حدوث المخاطر عند دراسة نظام المعلومات

✓ وبناءا عليه الفرضية الثالثة محققة جزئيا

4 -الفرضية الرابع : " هناك تفاوت في إمكانية نظام الأمن الإلكتروني في الحد من المخاطر بين المؤسسات محل الدراسة، و ترجع أسباب حدوث المخاطر التي تهدد نظم المعلومات في المؤسسة : أسباب تتعلق بموظفي المؤسسة نتيجة قلة الخبرة والوعي الأمن الإلكتروني، أسباب تتعلق بإدارة المؤسسة نتيجة لعدم سياسات واضحة والإجراءات الرقابية المطبقة"

✚ أولا: مؤسسة سونلغاز :

بالرجوع إلى نتائج الاستبيان يتبين أن درجة تكوين مستوعبة من طرف الأفراد العاملين على نظام المعلومات و بالمخاطر المحدقة بنظم المعلومات بأنها متوسطة إلى قليلة جدا بالنسبة 41,3، وأن توافر سياسات أمنية عالية مطبقة على مستوى المكونات المادية والبرمجية لنظام المعلومات ومقدرة بمتوسط 2,17 وهذا من شأنه يوحي إلى إن السياسات والإجراءات المطبقة غير كافية وبالتالي وفي حالتنا هاته نجد أن الأفراد العاملون على نظم المعلومات لا يتمتعون بدرجة الوعي الكافي ناحية المخاطر في حال العمل في بيئة ذات سياسات أمنية متوسطة وقد يعود ذلك إلى التقصير في إعلام هؤلاء الأفراد بواسطة التعليمات والمنشورات وتدريب المتخصص في إجراءات أمنية , و يرجوع إلى معامل الارتباط نجد إن السياسات والإجراءات الأمنية المطبقة بموظفي المؤسسة الذين هم يتصفون بقله الخبرة والوعي الأمن الإلكتروني و بإدارة المؤسسة نتيجة لعدم سياسات واضحة والإجراءات الرقابية المطبقة

✚ ثانيا :مؤسسة اتصالات الجزائر :

بالرجوع إلى نتائج الاستبيان يتبين أن درجة تكوين مستوعبة من طرف الأفراد العاملين على نظام المعلومات و بالمخاطر المحدقة بنظم المعلومات بأنها متوسطة إلى مرتفعة بالنسبة 39,2، وأن توافر سياسات أمنية عالية مطبقة على مستوى المكونات المادية والبرمجية لنظام المعلومات ومقدرة بمتوسط 2,38 وهذا من شأنه يوحي إلى إن السياسات والإجراءات المطبقة كافية وبالتالي وفي حالتنا هاته نجد أن الأفراد العاملون على نظم المعلومات يتمتعون بدرجة الوعي الكافي ناحية المخاطر في حال العمل في بيئة ذات سياسات أمنية متوسطة وقد يعود ذلك إلى التقصير في إعلام هؤلاء الأفراد بواسطة التعليمات والمنشورات وتدريب المتخصص في إجراءات أمنية , و يرجوع إلى معامل الارتباط نجد إن السياسات والإجراءات الأمنية المطبقة بموظفي المؤسسة الذين هم يتصفون بقله الخبرة والوعي الأمن الإلكتروني و بإدارة المؤسسة نتيجة لعدم سياسات واضحة والإجراءات الرقابية المطبقة

ثالثا :مؤسسة ليند غاز :

بالرجوع إلى نتائج الاستبيان يتبين أن درجة تكوين مستوعبة من طرف الأفراد العاملين على نظام المعلومات و بالمخاطر المحدقة بنظم المعلومات بأنها متوسطة إلى قليلة جدا بالنسبة 41,3, وأن توافر سياسات أمنية عالية مطبقة على مستوى المكونات المادية والبرمجية لنظام المعلومات ومقدرة بمتوسط 2,17 وهذا من شأنه يوحي إلى إن السياسات والإجراءات المطبقة غير كافية وبالتالي وفي حالتنا هاته نجد أن الأفراد العاملون على نظم المعلومات لا يتمتعون بدرجة الوعي الكافي ناحية المخاطر في حال العمل في بيئة ذات سياسات أمنية متوسطة وقد يعود ذلك إلى التقصير في إعلام هؤلاء الأفراد بواسطة التعليمات والمنشورات وتدريب المتخصص في إجراءات أمنية , ورجوع إلى معامل الارتباط نجد إن السياسات والإجراءات الأمنية المطبقة بموظفي المؤسسة الذين هم يتصفون بقلة الخبرة والوعي الأمن الالكتروني و بإدارة المؤسسة نتيجة لعدم سياسات واضحة والإجراءات الرقابية المطبقة

✓ وبناءا عليه الفرضية الرابعة محققة جزئيا

ثانيا : نتائج البحث :

اعتماداً على الإطار النظري للدراسة ونتائج الاختبارات الإحصائية، فقد خلصت الدراسة إلى العديد من النتائج والتي كان من أهمها:

- ❖ تتميز نظم المعلومات المؤسسات محل الدراسة من كفاءة في المكونات المادية والبرمجية .
- ❖ لدى مؤسسة ليند غاز نظم الأمن الكتروني يشمل كل العناصر لحماية أنظمتها من كل أنواع الاختراق
- ❖ لدى مؤسستي سونلغاز واتصالات الجزائر نظم الأمن يشمل كل عناصر .
- ❖ لدى مؤسستي سونلغاز واتصالات الجزائر نظم الأمن الكتروني لا تحميها من مخاطر نظم المعلومات .
- ❖ لدى مؤسسة ليند غاز نظام الكتروني فعال ويحميها ويحد من مخاطر نظم المعلومات
- ❖ هناك تفاوت في إمكانية نظام الأمن الالكتروني في الحد من المخاطر بين المؤسسات محل الدراسة
- ❖ هناك الخبرة ووعي كبير لدى الموظفين ليند غاز في الأمن الكتروني .
- ❖ نقص الخبرة والوعي لدى الموظفين سونلغاز واتصالات الجزائر في الأمن الكتروني بسبب قلة تحسيس وتكوين
- ❖ ترجع أسباب حدوث المخاطر التي تهدد نظم المعلومات في المؤسسة
- ❖ عدم وجود السياسات واضحة والإجراءات الرقابية المطبقة ومكتوبة في المؤسسات .
- ❖ إدراك الإدارة العليا بأهمية النظام الأمن الكتروني من ناحية تكوين الأفراد في مجال الأمن الكتروني ومشاركتهم في
- ❖ نجاعة نظام لدى مؤسسة ليند غاز
- ❖ عدم تطبيق إجراءات عقابية صارمة على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في
- ❖ مؤسستي سونلغاز واتصالات الجزائر

ثالثا : التوصيات :

بعد استعراض نتائج الدراسة فإنه يمكننا الخروج بمجموعة من التوصيات وهي كالآتي:

- ❖ من الضروري أن تدعم الإدارة العليا المؤسسات أمن المعلومات لديها وتعمل على إنشاء قسم خاص بتكنولوجيا المعلومات
- ❖ إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المؤسسات بحيث يكون له مشرفون في كل الفروع ذوي خبرة وكفاءة عالية من أجل العمل على حماية أمن معلومات.
- ❖ ضرورة امتلاك الإدارة العليا رؤيا والإستراتيجية واضحة لأمن نظم المعلومات داخل المؤسسة وسهر على بلوغها
- ❖ تطوير الشبكة في ظل الإمكانيات المتاحة، لأنها تعتبر القاعدة الأساسية لنظام المعلومات.
- ❖ يجب على الإدارة العليا إدراك بان نظام الأمن الكتروني هو بنية تحتية أساسية لازدهار مؤسسة وليست وسيلة مساعدة الثانوية كما هو متعارف عليه في الواقع .
- ❖ وضع إجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها وتقليل من احتمال وقوعها.
- ❖ ضرورة مراقبة عملية الصيانة للأجهزة والبرامج، على أن تكون هذه العملية دورية ومنتظمة وداخلية ؛
- ❖ وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أو اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية
- ❖ يجب على المؤسسة تطبيق إجراءات عقابية صارمة على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات

رابعا :أفاق البحث :

حاولنا من خلال هذه الدراسة إبراز أثر نظام الأمن الكتروني في الحد من مخاطر النظم المعلومات بما يستجيب لمتطلبات متخذي القرارات في مؤسسات محل الدراسة ، في تحقيق ذلك بجملة من الاختبارات لتحليل آراء مستخدمي النظام ، لكن هناك مجالات في الدراسة تحتاج إلى اهتمام بمهدف تغطية جوانب و إثراء المقارنة بقطاعات أخرى أهمها :

- ❖ أثر تطبيق سياسات أمن المعلومات على الأمن التنظيمي في الجامعات الجزائرية :
- ❖ مدى مساهمة نظام الأمن الكتروني في الحد من المخاطر نظم المعلومات في قطاع النفط.
- ❖ قياس تكلفة تطبيق المعايير الدولية لأمن المعلومات في مؤسسات الحكومية الجزائرية .
- ❖ تقييم إستراتيجية نظم المعلومات في عينة من المؤسسات



المراجع



أولا : المراجع باللغة العربية

الكتب :

1. أبو بكر محمود الهوش ، "نظم وشبكات المعلومات، مؤسسة الثقافة الجامعية"، مصر، 2007.
2. أحمد فتحي الحيت، مبادئ الإدارة الالكترونية، دار الحامد للنشر والتوزيع، عمان، 2015
3. سعد غالب ياسين ،"نظم المعلومات الإدارية وتكنولوجيا المعلومات"، دار المناهج، عمان، 2012
4. عبد الرزاق محمد قاسم، تحليل وتصميم نظم المعلومات المحاسبية، دار الثقافة، دمشق، 2009
5. علاء محمد شوقي إبراهيم عيسى ،تأثير تطبيق حوكمة الشركات على مخاطر نظم المعلومات المحاسبية ، دار الجزائرية للنشر والطبع والتوزيع، الجزائر، 2015
6. علاء حسين الحمامي، سعد عبد العزيز العاني ، "تكنولوجيا أمنية المعلومات و أنظمة الحماية"، دار وائل، الأردن، 2007.
7. كمال الدين مصطفى الدهراوي، نظم المعلومات المحاسبي في ظل تكنولوجيا المعلومات، المكتب الجامعي الحديث، مصر، 2009
8. محمد الصيرفي، نظم المعلومات الإدارية ، طبعة الأولى، مؤسسة حورس الدولية، الإسكندرية، 2005
9. مروان العبد محمد أبو زعنونة و علاء الدين محمد الصويطي، "مقدمة في أمن الشبكات"، دار المعتز، الأردن، 2009.
10. هويدا علي عبدالقادر، "نظم المعلومات الإدارية النظرية والتطبيق"، دار الجنان للنشر والتوزيع، الخرطوم، 2011.

البحوث العلمية :

1. أمل ابراهيم أبو رحمة، نظام معلومات الموارد البشرية وأرها على فاعلية ادارة شؤون الموظفين في فلسطين، مذكرة ماجستير، ادارة الأعمال، غزة 2005
2. أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية، أطروحة ماجستير، كلية التجارة، غزة، 2013
3. أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية، أطروحة ماجستير، كلية التجارة، غزة، 2013
4. حرية شعبان الشريف، "مخاطر نظم المعلومات المحاسبية الإلكترونية :دراسة تطبيقية على المصارف العاملة في قطاع غزة"، مذكرة ماجستير، الجامعة الإسلامية غزة، 2006.

5. خالد رجم ، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2017
6. قدور مقراني، تقييم مدى مساهمة نظام الامن الالكتروني في الحد من المخاطر نظم المعلومات ، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2016
7. محمد الطاهر الأخضر، أثر نظام المعلومات المحاسبي الإلكتروني على الخصائص النوعية للمعلومات المحاسبية، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2016
8. يزيد ذكار ،تقييم كفاءة نظام المعلومات الالكتروني ،مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة، 2016

المقال المنشور :

1. عصام محمد البحيصي و حرية شعبان الشريف، "مخاطر نظم المعلومات المحاسبية الالكترونية" ، مجلة الجامعة الإسلامية، غزة ، المجلد 16 ، العدد 2. 2007.

المحاضرات :

2. خالد رجم، ، "محاضرات أمن نظم المعلومات"، مقياس مراجعة نظام المعلومات، أولى ماستر، جامعة ورقلة، 2015-2016.

ثانيا : المراجع باللغة الأجنبية :

1- الكتب :

1- laudon & laudon-management information systems-the digital firm ,
dition9, Pearson Education, USA,2006

2- Oihab Allal-Chérif et Olivier Dupouet, « Optimisez votre Système
d'Information « vers la PME numérique en réseau » », Afnor,Saint-
Denis, France,2014

2- البحوث العلمية

1- MWITA SIMION MAROA, « Factors affecting information systems
security effectiveness in university of Nairobi »,Thesis of Master of
science degree in information systems, Kenya,2015.

2- Robert Reix , système d'information et management desorganisation ,
édition 5 vuibert –gestion , paris , France

3- Robert Reix, Bernard Fallery, Michel Kalika et Frantz Rowe,
« Système d'information et gestion des organisations », 6 edition,
Vuibert, paris , 2011.

3- مواقع الانترنت

- ✓ <http://asca.sy/download/PDF/murajaa-pdf.pdf>
- ✓ <http://www.accdiscussion.com/t12332>
- ✓ <https://sqarra.wordpress.com/inaudit/>



الملاحق



الملحق رقم (1): أسئلة المقابلة

01. ما هو المسمى الفعلي للقسم المسئول المباشر عن نظم المعلومات ؟
02. متى تأسس القسم ؟ وما هي مراحل تطوره ؟ نبذة تاريخية.,.
03. ما هي الرؤية، الرسالة، والغايات، وما هي الخدمات التي تقدمونها؟
04. وهل هناك خطط إستراتيجية لمؤسسة ؟
05. كم عدد الموظفين في المؤسسة ؟ وما طبيعة الهيكل الإداري المؤسسة ؟ هل من الممكن تزويدنا بها ؟

❖ هل توجد جهة مختصة بأمن المعلومات ؟

06. شخص موكل له القيام بقضايا أمن المعلومات ومتابعتها ؟ وما هي المعوقات لفعل ذلك ؟
07. هل يعتبر أمن المعلومات أولوية بالنسبة لكم ؟ وكيف ترون متطلبات الأمن (السرية – التوفر السلامة) بالنسبة لأنشطة المعلومات

❖ هل لديكم سياسة أمن معلومات؟

08. ما هي البنية التحتية لتكنولوجيا المعلومات، بمعنى ما هو طبيعة نظم المعلومات ككل؟
09. هل تليي البنية التحتية الحالية لنظم المعلومات احتياجات الأقسام (المؤسسة) بمعنى هل الشبكة فعالة، هل البرمجيات ذات كفاءة ،

❖ هل الخوادم تعمل بشكل مناسب، هل يتم مراجعة دورية وفحص و إجراء تقييم للبنية التحتية؟

10. ماذا عن خطط الاستبدال لمكونات نظام المعلومات ؟ تكلم عن كل جزء بشكل منفرد:

المادي.

البرمجي

نظم تشغيل

برامج التطبيقات

الشبكي (وسائط النقل – الشبكة اللاسلكية – الموجهات والمبدلات-تحسين سرعة النقل –الربط

بالانترنت)

11. هل يتم إجمال التهديدات التي من الممكن التعرض لها وبدوره السؤال أشمل هل تقومون بإدارة وتحليل للمخاطر ؟ ما هي

الأنواع ونسب التهديدات من وجهة نظرك]

الثغرات الأمنية

التهديدات بأنواعها:

✚ التهديدات الغير متعمدة

✚ التهديدات المتعمدة

✚ التهديدات الطبيعية

✚ الأخطاء التقنية

✚ الأخطاء الإدارية

12. هل ترون في الموقع لقسم المشرف على الخوادم / نظم المعلومات موقعا مناسباً؟

13. ماذا عن وسائل الحماية المتبعة؟

✚ وسائل الحماية المادية

✚ وسائل الحماية الفنية (التقنية)

✚ ضبط الوصول

✚ التشفير

✚ وسائل الحماية التنظيمية (الإدارية)

✚ تصنيف المعلومات

✚ التوثيق

✚ النسخ الاحتياطي

✚ خطط الطوارئ والاسترداد الآمن

✚ خطط التطوير والتعلم من الأخطاء

14. ماذا عن التعهد؟ وهل ترون فيه حل؟ وما الفوائد؟ والمعوقات و العيوب؟

15. ما هي السبل التي يمكن اتخاذها لحماية المؤسسة من مخاطر قد تتعرض لها سلامة وتوفر المعلومات؟

الملحق رقم (2): استمارة الاستبيان



جامعة قاصدي مرباح - ورقلة

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم التسيير

استبيان مذكرة ماستر

أخي الموظف/أختي الموظفة

السلام عليكم ورحمة الله وبركاته، وبعد: يهدف هذا الاستبيان إلى التعرف على آرائكم فيما يختص بالمخاطر الهامة التي تواجه أمن نظم المعلومات الإلكترونية في مؤسساتكم، وهي بعنوان "تقييم مدى مساهمة نظام الأمن الإلكتروني في الحد من مخاطر نظم المعلومات"، بهدف استكمال متطلبات الحصول على درجة الماستر في علوم التسيير تخصص تدقيق والمراقبة التسيير. لذلك نرجو منكم التكرم بملء خانات الاستبيان المرفق، كما نؤكد لكم على أن البيانات التي سوف يتم تجميعها في هذا الاستبيان ولن تستخدم إلا لأغراض البحث العلمي فقط. نشكر لكم مشاركتكم و تعاونكم معنا مسبقا.

الباحث: بن عمارة الطاهر tahaer.benamara@gmail.com

تحت الإشراف الدكتور: رجم خالد

المحور الأول : المعلومات العامة

يرجى التكرم بوضع علامة (X) في الخانة المناسبة:

01-الجنس		ذكر		أنثى	
02-العمر		20 سنة إلى 30 سنة	30 سنة إلى 40 سنة	40 سنة إلى 50 سنة	50 سنة فأكثر
03-المستوى التعليمي		ابتدائي	متوسط	ثانوي	تقني جامعي
04- الخبرة		أقل من 5 سنوات	من 5 إلى 10 سنوات	من 10 إلى 15 سنة	من 15 إلى 20 سنة أكثر من 20 سنة
05-المؤهل العلمي		بكالوريا	ليسانس	ماستر	ماجستير تقني سامي غير ذلك حدد

لا			نعم			06- المؤسسة توافر إدارة لأمن نظم المعلومات
بصورة قليلة جدا	بصورة قليلة	بصورة متوسطة	بصورة مرتفعة	بصورة مرتفعة جدا	07-مدى استخدام المؤسسة لنظم المعلومات المحوسبة	
					08-مستوى التدريب الذي تتلقونه في مجال أمن المعلومات	
قليل جدا	قليل	متوسط	مرتفع	مرتفع جدا		

الرقم	مخاطر نظم المعلومات	لم يحدث أبدا	أحيانا	يحدث دائما
01	الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين.			
02	الإدخال المتعمد (المقصود) للبيانات غير سليمة بواسطة الموظفين.			
03	التدمير غير المتعمد (الحذف) للبيانات بواسطة الموظفين.			
04	التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين.			
05	المرور (الوصول) غير الشرعي للبيانات أو للنظام بواسطة الموظفين			
06	المرور غير الشرعي (غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة.			
07	تعرضت أجهزة الحاسوب في المؤسسات الى الفيروسات.			
08	تم تعديل بعض خصائص أو تدمير بنود معينة من المخرجات.			
09	خلق مخرجات زائفة / غير صحيحة.			
10	سرقة البيانات / المعلومات.			
11	عمل نسخ غير مصرح (مرخص) بها من المخرجات.			
12	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعا على الورق. (أي اطلاع موظفين أو أشخاص آخرين على مخرجات تم طبعا وهم غير مرخصين لذلك).			
13	تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.			

			تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية.	14
--	--	--	--	----

المحور الثاني: مخاطر نظم المعلومات.

فيما يلي عبارات متعلقة بموضوع الدراسة يرجى التكرم باختيار واقع المؤسسة التي تعمل بها ، وذلك بوضع علامة (X) في الخانة التي تناسب اختيارك.

المحور الثالث : نظام الأمن الكتروني في المؤسسة.

الرقم	البعد الأول : السياسات والإجراءات .	غير موافق	محايد	موافق
01	توجد في المؤسسة سياسات وإجراءات مكتوبة لأمن المعلومات.			
02	تدرك الإدارة أهمية سياسات أمن المعلومات.			
03	يتم مراجعة وتطوير سياسات أمن المعلومات بشكل دوري.			
04	يتم إدخال المعلومات بعد مصادقة الرئيس المصلحة المباشر.			
05	لا يسمح لغير المختصين بالوصول إلى الأجهزة والعتاد المحوسب.			
06	يمنع الدخول لمواقع الانترنت بأجهزة الموصولة بالخادم المركزي.			
07	لا يسمح بتثبيت البرامج غير الأصلية (الغير المرخصة) و المقرصنة.			
08	يتم تجديد العتاد دوريا.			
09	يفرض على الموظفين تغيير كلمة المرور دوريا			
10	يتم التصريح بعناوين الحواسيب IP حتى يتم الدخول النظام			
11	تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها			
الرقم	البعد الثاني : إجراءات امن المعلومات المتعلقة بالعمالين .	غير موافق	محايد	موافق
12	يتوافر تدريب للعمالين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.			
13	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة			
14	يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص			

			المؤسسة كجزء من شروط التوظيف.
15			يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.
16			هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.
17			يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة.
18			لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا.
الرقم	غير موافق	محايد	موافق
19			تستخدم المؤسسة شتى الوسائل (أبواب - أقفال - بطاقات دخول - كاميرات) لحماية مكونات نظم المعلومات .
20			يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها.
21			يمنع الموظف الغير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.
22			كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها.
23			تستخدم طرق تشفير لحماية البيانات.
24			توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن.
25			توجد برامج حماية لتتبع ومنع الاختراق والتسلل.
26			تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.
27			يتم تثبيت مضادات الفيروسات والتحديثات الدورية .
28			يتم صيانة الشبكة والعتاد دوريا.

شكرا جزيلاً لتعاونكم .

الملحق رقم (3): واجهة نظام المالي ومحاسبي



Comptabilité générale

Comptabilité analytique

Gestion des immobilisations

Gestion des investissements

Gestion des règlements

Administration système

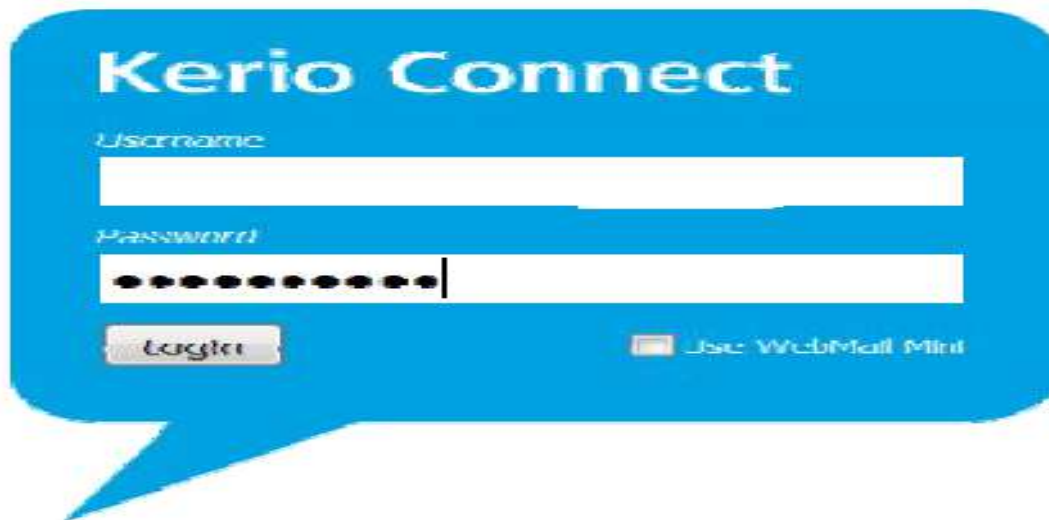
Bienvenue (m.lakhdar)

© Copyright 2012, ELIT, Tous Droits Réservés.

المصدر: نظام المعلومات الالكتروني سونلغاز

الملحق رقم (4)

واجهة تقنية الاتصال للبريد الداخلي المحلي Kerio Connect



Kerio Connect

Username

Password

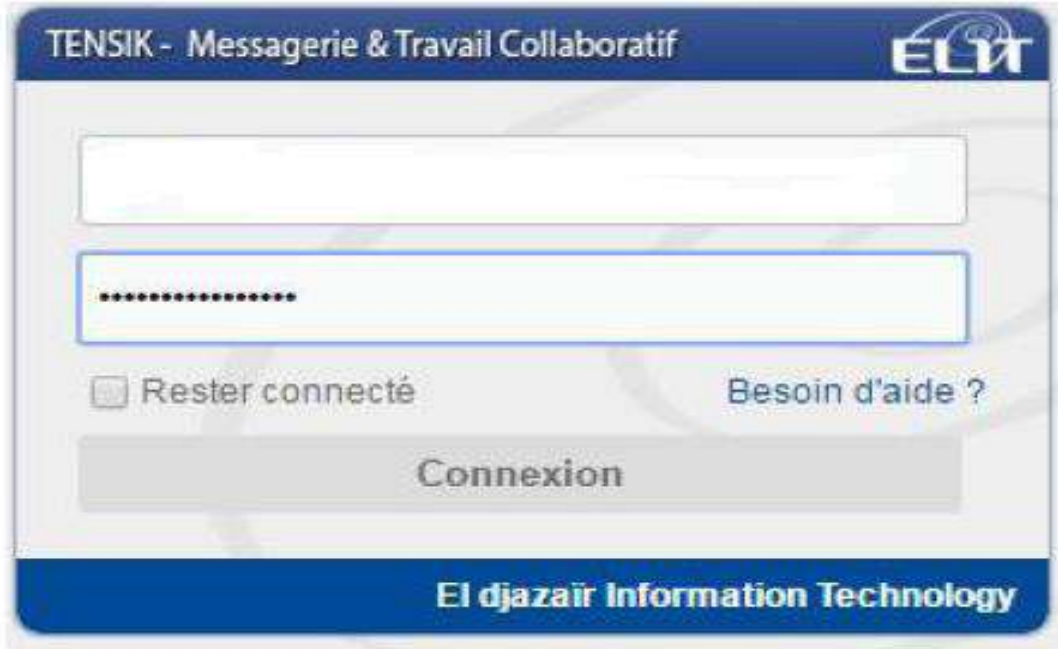
Login

Use WebMail Mini

المصدر: نظام المعلومات الالكتروني سونلغاز

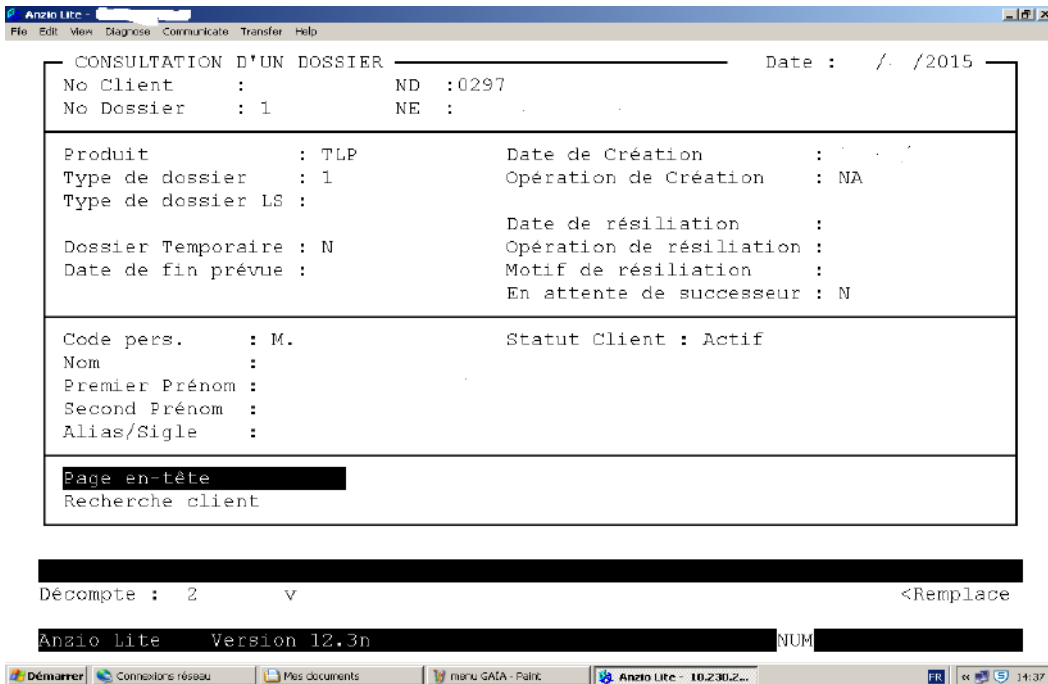
الملحق رقم (5)

واجهة تقنية الاتصال للبريد الداخلي الواسع TENSİK



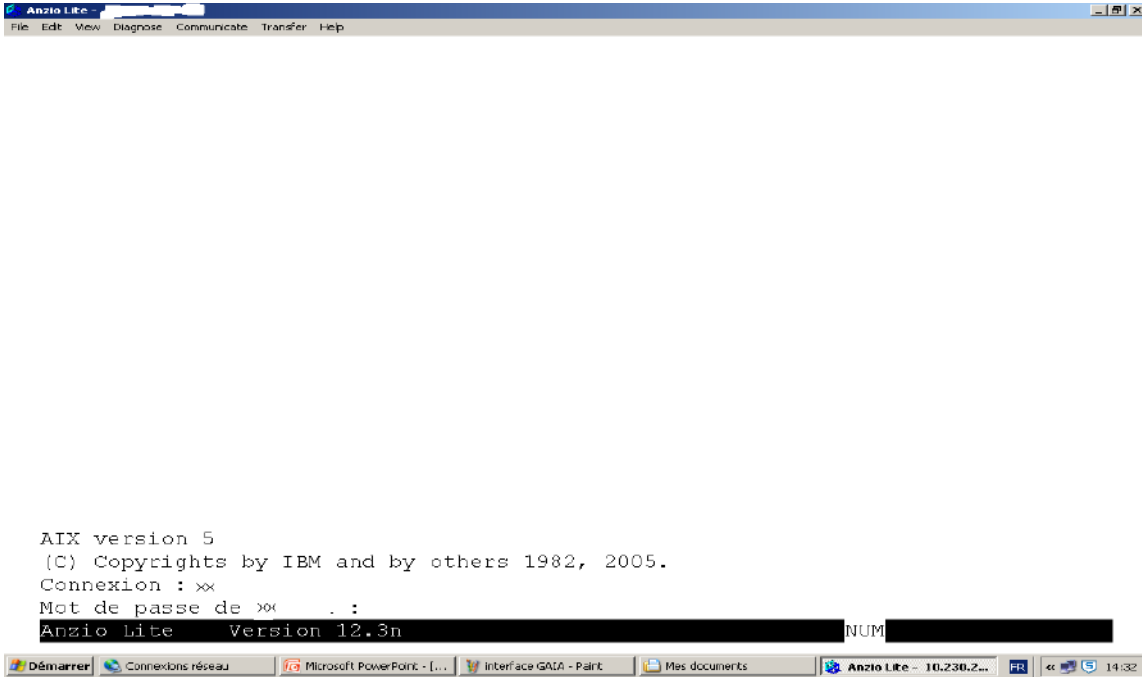
المصدر: نظام المعلومات الالكتروني سونلغاز

الملحق رقم (6) نافذة من البرنامج



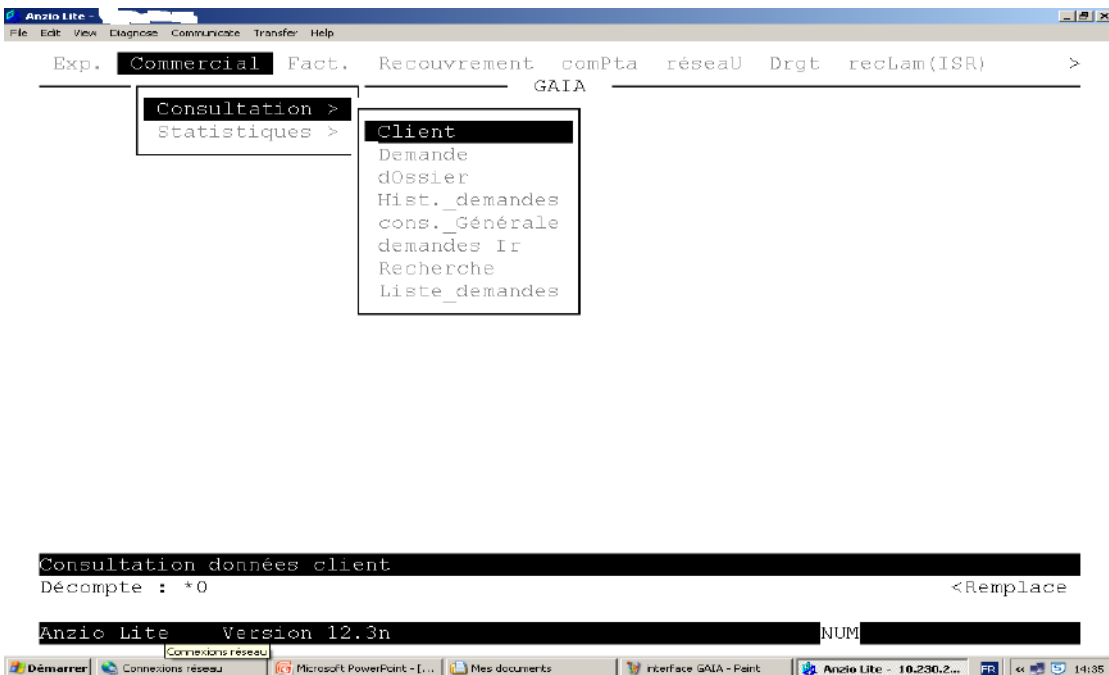
المصدر: نظام المعلومات الالكتروني اتصالات الجزائر

الملحق رقم (7) نافذة الدخول للبرنامج

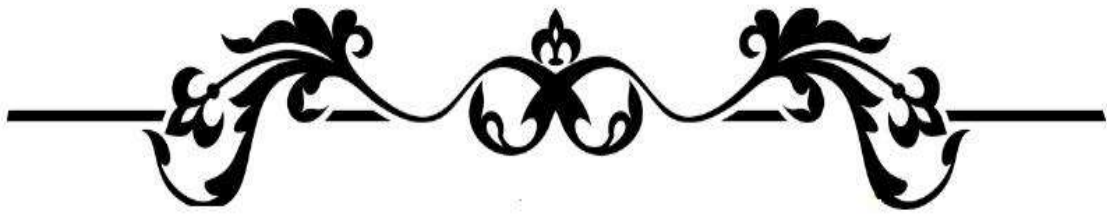


المصدر: نظام المعلومات الالكتروني اتصالات الجزائر

الملحق رقم (8): قائمة البرنامج



المصدر: نظام المعلومات الالكتروني اتصالات الجزائر



الفهرس



الصفحة	العنوان
III	الإهداء
IV	الشكر
V	الملخص
VI	قائمة المحتويات
VII	قائمة الجداول
VIII	قائمة الأشكال
X	قائمة الاختصارات والرموز
IX	قائمة الملاحق
ب	المقدمة
01	الفصل الأول : الأدبيات النظرية و التطبيقية لمساهمة نظام الأمن الالكتروني في الحد من مخاطر نظام المعلومات
03	المبحث الأول : الإطار النظري لمخاطر نظم المعلومات الالكترونية
03	المطلب الأول: عموميات حول نظام المعلومات
03	الفرع الأول: ماهية نظام معلومات
05	الفرع الثاني: عناصر نظام معلومات
06	الفرع الثالث: أنواع نظم معلومات حسب مستويات التسيير
08	الفرع الرابع: أهداف نظام المعلومات
09	المطلب الثاني: الأمن نظام المعلومات
09	الفرع الأول: ماهية أمن المعلومات
10	الفرع الثاني:عناصر أمن المعلومات
11	الفرع الثالث: متطلبات أمن نظم المعلومات
11	الفرع الرابع: تصميم نظام الأمن
12	المطلب الثاني: مخاطر وتهديدات نظام المعلومات
13	الفرع الأول: ماهية المخاطر نظم المعلومات
14	الفرع الثاني: المخاطر نظم المعلومات
19	الفرع الثالث:أسباب حدوث المخاطر نظم المعلومات
19	الفرع الرابع: تهديدات نظم المعلومات
23	المبحث الثاني: الدراسات السابقة

23	المطلب الأول: الدراسات السابقة باللغة العربية
24	المطلب الثاني : الدراسات السابقة باللغة الأجنبية
26	المطلب الثالث: مقارنة الدراسة الحالية بالدراسات السابقة
26	الفرع الأول: أوجه التشابه
26	الفرع الثاني : أوجه الاختلاف
28	الفصل الثاني : الدراسة الميدانية لتقييم اثر الأمن الالكتروني على الحد من المخاطر النظم المعلومات
29	المبحث الأول : الطريقة والأدوات المستخدمة في الدراسة
29	المطلب الأول : عينة الدراسة
29	الفرع الأول :المجتمع وحجم عينة الدراسة
32	الفرع الثاني :تعريف المؤسسات محل الدراسة
32	المطلب الثاني : الأدوات المستخدمة الدراسة
32	الفرع الأول : الأدوات المستخدمة في الدراسة
33	المطلب الثالث : تحليل واقع النظام الأمن الالكتروني في المؤسسة
33	الفرع الأول :مكونات نظام المعلومات المؤسسة :
41	الفرع الثاني : السياسات الأمنية المتبعة
45	المبحث الثاني :النتائج المتحصل عليها ومناقشتها
45	المطلب الاول :النتائج الاستبيان
45	الفرع الاول : الطريقة المستخدمة في القياس
47	الفرع الثاني:تحليل وصفي لخصائص الديمغرافية لعينة الدراسة
56	الفرع الثالث :قياس اتجاه أفراد العينة نحو عبارات الاستبيان
77	الفرع الرابع : معامل سبيرمان للارتباط
78	المطلب الثاني :المناقشة النتائج
78	الفرع الأول :المناقشة
80	الفرع الثاني : المقارنة بين السياسات الأمنية عينة الدراسة
81	الفرع الأول : مدى إمكانية حدوث مخاطر نظام المعلومات
84	الخاتمة
92	المراجع
96	الملاحق

106	الفهرس
-----	--------