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 أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم المعلومات

دراسة حالة مؤسسة اتصالات الجزائر

من إعداد الطالب: قدور مقراني

نوقشت وأجيزت علنا بتاريخ :2016/05/24

أمام اللجنة المكونة من السادة:

الأستاذ(ة)/ أسماء يوسف.....(أستاذ- جامعة قاصدي مرباح ورقلة) رئيسا
الدكتور/ محمد الأمين شربي.....(أستاذ- جامعة قاصدي مرباح ورقلة) مشرفا ومقررا
الأستاذ/ خالد رجم.....(أستاذ- جامعة قاصدي مرباح ورقلة) مناقشا

السنة الجامعية : 2015 – 2016

الإهداء

أهدي ثمرة هذا

الجهد، إلى كل من أدين

له بلحظة سعادة.

الشكر والعرفان

الحمد لله الذي بنعمته تتم الصالحات، أتقدم بالشكر إلى كل من ساعدني من قريب أو من بعيد لإنجاز هذا العمل، وأخص بالذكر المؤطر، الدكتور والأخ : شربي محمد الأمين، كما أشكر زملائي في الدفعة كل بإسمه، ولا أنسى أساتذتنا الأفاضل الذين لم يبخلوا علينا بالنصائح تارة، وبالتشجيع لمواصلة الدرب تارة أخرى، وكما أتقدم بشكر خاص إلى العائلة الكريمة التي وفرت لي الجو الملائم لمواصلة الدراسة ، أمي ، وزوجتي العزيزة ، والمشاغب الصغير "خذيفة".

إليكم جميعا، شكرا جزيلا.

الملخص :

هدفت هذه الدراسة إلى تقييم أمن نظام المعلومات في مؤسسة إتصالات الجزائر، حيث تطرقت إلى المخاطر المحيطة بنظام المعلومات والإجراءات التي من شأنها الحد من هذه المخاطر، ومن ثم محاولة إسقاط هذه المعطيات على نظام المعلومات داخل المؤسسة المعنية بالدراسة، وقد اعتمدنا على المنهج الوصفي في الجانب النظري من أجل تسليط الضوء على نظم المعلومات ومخاطرها والعناصر الأمنية، وأثناء إعداد هذه الدراسة قمنا بتوزيع الاستبيان الذي تمثل في توزيع 100 استمارة، وقد تم استرداد 90 استمارة، وقد بلغ معدل الاستجابة 90 % و كانت 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.

الكلمات المفتاحية: نظام معلومات ، أمن نظم معلومات، مخاطر نظم معلومات، اتصالات الجزائر.

Abstract :

This study aimed at the evaluation of the information security system at “Algerie Telecom” company, it reported the threats staring at the information system and the measures that may reduce these risks, and then attempted to project these facts on the information system within the company.

We adopted a descriptive approach in the theoretical side in order to reveal the information systems, their risks and the security elements.

During the preparation of this study, we distributed a 100 copy of a questionnaire, 90 copies has being recovered. 90% was the response rate, from the answers we concluded that the security policies within the information system are able to ensure the continuity of work in this system in optimal conditions involving the human factor in these policies.

Key words: Information system, Information systems security, Information systems threats, Algerie Telecom.

-قائمة المحتويات-

قائمة الجداول

قائمة الأشكال

قائمة الملاحق

قائمة المختصرات

الاختصار	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
ERSBSUD	Etablissement Régional de Système & Billing SUD	الهيئة الجهوية للأنظمة و الفوترة للجنوب
CRM	Client Relationship Management	تسيير العلاقات مع الزبائن
RMS	Reseau Multi Service	شبكة متعددة الخدمات
LAN	Local Area Network	الشبكة المحلية
IP	Internet Protocol	بروتوكول أنترنت
TCP	Transmission Control Protocol	بروتوكول التحكم بالنقل
VPN	Vitual Private Network	الشبكة الخاصة الإفتراضية
SPSS	Statistical Package for the Social Sciences	الحزمة الإحصائية للعلوم الاجتماعية

المقدمة

- **توطئة :**

أصبحت المؤسسات على اختلاف أنماطها تعتمد على أنظمة المعلومات المختلفة إن كانت معقدة أو بسيطة، وتعتبر هذه الأنظمة العمود الفقري للمؤسسة لإمدادها بالمعلومة المناسبة، ومع التطور التكنولوجي في جميع الميادين وبالأخص في ميدان الاتصالات، أصبحت أنظمة المعلومات مبنية أساسا على قواعد تكنولوجية، انطلاقا من عملية الإدخال ومرورا بعملية المعالجة، وصولا إلى المخرجات والتغذية العكسية.

ولقد وفرت التكنولوجيا اختزال الوقت والجهد والمصاريف، ولكن بالمقابل، ازدادت المخاطر المحدقة بأنظمة المعلومات في بيئة متقلبة ومفتوحة على العالم، من هنا كان لابد على المؤسسة أن تشدد إجراءاتها الأمنية لحماية أنظمتها المعلوماتية، وانطلاقا من هذا الطرح وفي إطار دراسة وتقييم أمن نظم المعلومات الإلكترونية وتأثيره في الحد من المخاطر المحتملة على نظم المعلومات ، يطرح التساؤل التالي:

ما مدى مساهمة أمن نظام المعلومات الالكتروني في الحد من مخاطر نظام المعلوماتفي مؤسسة اتصالات الجزائر بورقلة؟

وتندرج تحت هذه الإشكالية الرئيسية، إشكاليات فرعية تتمثل في الآتي:

1 -ما هي أنواع المخاطر التي تهدد نظام المعلومات ؟؛

2 -هل تؤثر السياسات الأمنية على المكونات المادية والبرمجية لنظم المعلومات؟؛

3 -كيف تؤثر السياسات الأمنية على الموظفين العاملين على نظم المعلومات؟؛

- **الفرضيات:**

1 -تتعدد المخاطر التي تهدد نظام المعلومات بحسب مراحل النظام في حد ذاته ، فهنا ك مخاطر متعلقة بعمليات الإدخال، المعالجة و المخرجات؛

2 -تسمح السياسات الأمنية بزيادة أداء المكونات المادية والبرمجية ودعمومة عمل نظام المعلومات لنظم المعلومات؛

3 -يتمتع الأفراد العاملون على نظم المعلومات بدرجة وعي أكبر ناحية المخاطر في حال العمل في بيئة ذات سياسات أمنية عالية.

- **مبررات اختيار الدراسة:**

-الميول الشخصية للباحث من لهاته المواضيع؛

-المشاكل التي تعاني منها المؤسسات في جانب الأمن الإلكتروني؛

-التطور المتسارع في تكنولوجيات أمن المعلومات؛

-قيمة وأهمية الموضوع وإمكانية مواصلة البحث فيه.

- **الأهمية:**

يستمد الموضوع أهميته من كون أن المؤسسات تتجه نحو الاعتماد على نظم معلومات إلكترونية، مما يجعلها عرضة لمخاطر عدة، هذه المخاطر تهدد استمرارية المؤسسة وأدائها.

- **الهدف :** تهدف الدراسة إلى:

- التعرف على أنواع المخاطر التي تواجه نظم المعلومات؛

- التعرف على السياسات الأمنية المتبعة للحد من هذه المخاطر؛

- قياس درجة العلاقة بين السياسات الأمنية والحد من مخاطر نظم المعلومات.

- **حدود الدراسة :**

-الحدود المكانية: تم اختيار مؤسسة إتصالات الجزائر المفوضية الجهوية لاتصالات الجزائر بورقلة، ويرجع ذلك إلى موضوع الدراسة حيث أن نظام المعلومات يتناسب بشكل كبير مع نشاط هذه المؤسسة والتي تشتغل في بيئة تكنولوجية متغيرة بسرعة.

-الحدود الزمنية :تمت هذه الدراسة خلال الثلاثي الأول لسنة 2016.

- **المنهج المتبع:**

لقد تم الاعتماد على المنهج الوصفي للإجابة على التساؤلات وإثبات فرضيات الدراسة ، أما في الجانب التطبيقي فلقد تم استعمال أسلوب دراسة الحالة كما تم الاستعانة أيضا بأدوات البحث و المتمثلة في: الملاحظة، المقابلة والاستبيان.

- **صعوبات الدراسة:**

تمثلت صعوبة الدراسة، في طبيعة المعلومات المراد جمعها كون البحث له جانب تقني وجانب إداري، كما كان لسرية المعلومات أيضا الأثر الكبير في إنجاز هذا البحث.

- **هيكل الدراسة :**

من أجل معالجة الإشكالية المطروحة واختبار الفرضيات، تمت هيكلة الموضوع بالبدء بمقدمة الموضوع، ثم تقسيم الدراسة إلى فصلين ، تناول الفصل الأول الأدبيات النظرية والتطبيقية للدراسة ، وهو بدوره قسم لمبحثين، المبحث الأول بعنوان الأدبيات النظرية للدراسة وتطرق المبحث الثاني للدراسات السابقة المتعلقة بموضوع الدراسة، أما الفصل الثاني فجسد الجانب التطبيقي للدراسة من خلال إجراء دراسة الحالة وقسم بدوره إلى مبحثين ، المبحث الأول يتطرق إلى الطريقة المستعملة والأدوات المستخدمة في البحث ، أما المبحث الثاني فخصص لعرض النتائج المتوصل إليها ومناقشة النتائج ، وفي نهاية البحث حوت الخاتمة على ملخصا عن الدراسة ونتائجها وأهم التوصيات.

الفصل الأول:

الأدبيات النظرية والتطبيقية لمخاطر وأمن نظام

تمهيد :

تنشط المؤسسات في بيئة داخلية وخارجية معقدة، يستوجب منها التأقلم مع كل المستجدات التكنولوجية من أجل الحفاظ على إستمراريتها وتحقيق أهدافها، وحتى تصل إلى هذه الغاية يجب على هذه المؤسسات أن تمتلك نظام معلومات كفؤ وفعال يمكنها من الحصول على المعلومات اللازمة في الوقت المناسب، من هنا تظهر مدى أهمية نظام المعلومات في نشاط المؤسسة.

إن نظام المعلومات يعتبر اللبنة الأساسية داخل المؤسسة، لذلك وجب على المسيرين الاهتمام به في ظل وجود مجموعة من المخاطر والتهديدات المحيطة به والتي من شأنها إعاقة السير الحسن له، وحتى يمكن السيطرة على هذه المخاطر كان لزاما على المؤسسة اتخاذ إجراءات وسياسات أمنية، وقائية كانت أو علاجية.

وبناء على ما تقدم، سيتم تقسيم هذا الفصل إلى مبحثين، المبحث الأول سنتناول فيه المفاهيم العامة المتعلقة بنظام المعلومات والمخاطر والتهديدات المحيطة به ومن ثمة سنتناول الإجراءات الأمنية الواجب إتباعها، أما المبحث الثاني فسنتطرق فيه إلى الدراسات السابقة التي لها علاقة بهذه الدراسة.

المبحث الأول: الأدبيات النظرية

يعتبر نظام المعلومات من المقومات التسييرية داخل المؤسسة، حيث يعتمد عليه في جميع نشاطات المؤسسة من أجل دعم أنشطتها لغرض تحقيق أهدافها المسطرة، وسيتم خلال هذا الجزء من البحث التعرف على ماهية نظم المعلومات، وما هي المخاطر المحدقة به وكذا السياسات الأمنية المتبعة من أجل الحد من هذه المخاطر.

المطلب الأول: ماهية نظام المعلومات

في هذا المطلب سوف نتطرق إلى بعض المفاهيم النظرية حول نظام المعلومات ، ومكوناته ووظائفه.

أولا: تعريف نظام المعلومات

تعرف على أنها مجموعة منظمة من المصادر: المادية، البرامج، البشرية، المعطيات و الإجراءات التي تسمح بتجميع، معالجة وتخزين المعلومات (على شكل بيانات، نصوص، صور،صوت، ... الخ) داخل وبين المنظمات[1].

وفي تعريف ثان هو مجموعة من الأشخاص، الإجراءات والمصادر التي تجمع المعلومة، وتحولها وتوزعها داخل المنظمة [2].

أما "نادية لونيس" فتعرفه على أنه هو النظام الذي يتكون من مجموعة من الأجزاء (المعلومات، الأفراد، التجهيزات و الإجراءات) المترابطة، والتي تعمل معا بشكل متناسق من خلال مجموعة من العمليات المنتظمة (تجميع، تخزين، معالجة وتحليل)، وعرض المخرجات والنتائج بالأشكال المختلفة للمعلومات (تقارير، أشكال، رسومات و مخططات) بحيث تزود النتائج للمستفيدين من هذا النظام بطريقة تدعم وتخدم قراراتهم وتسهل أعمالهم وتمكنهم من التخطيط والرقابة على نشاطات المؤسسة[3].

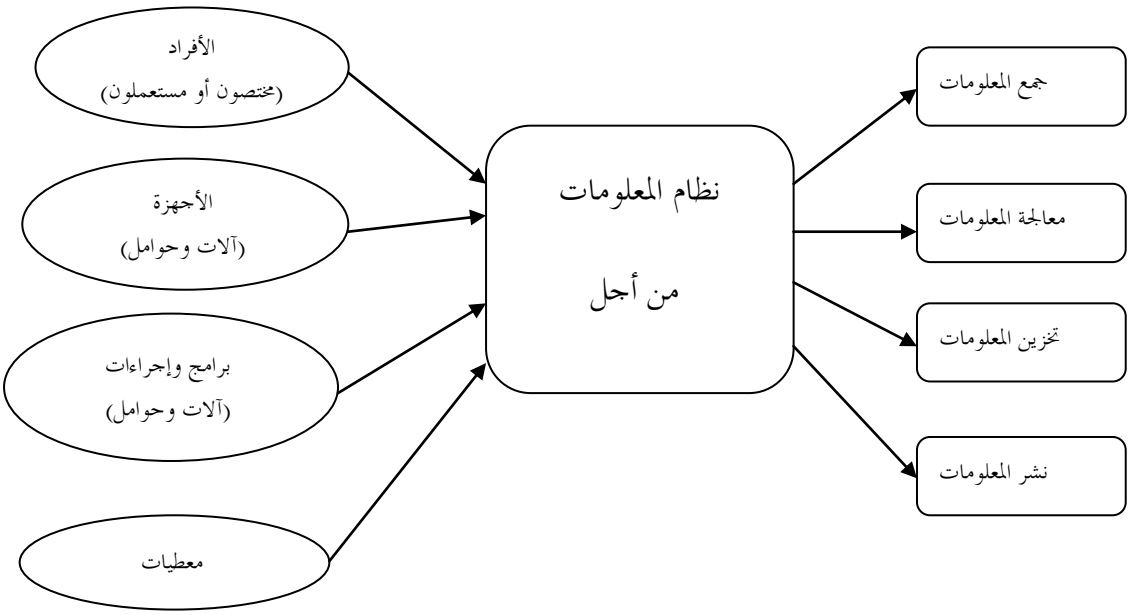
ويعرفه هويدا علي عبد القادر بـــ: "هو ذلك النظام الذي يستخدم الأفراد والمعدات والإجراءات وسياسات التشغيل لتجميع ومعالجة البيانات وتوزيع المعلومات ، بمعنى آخر، نظم المعلومات مصطلح يدل على

[1] Stéphane Bourliataux, Cyril Gallitre & Yvers Roy, **« Systèmes d'information de gestion »**, Dunod, Paris, 2008, p :6.
[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] لونيس نادية، **"أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات"** مذكرة ماجستير غير منشورة، جامعة الجزائر3، 2011/2010، ص: 12.

نظام يقوم بجمع المعلوم ات (يدويا أو آليا) وتنظيمها وتخزينها ومعالجتها وعرضها في أشكالها المختلفة (نصية، مرئية، صوتية)"[1].

يوضح الشكل التالي مكونات نظام المعلومات :

الشكل 1-1: مكونات نظام المعلومات



Source : Robert Reix, Bernard Fallery, Michel Kalika et Frantz Rowe, Système d'information et gestion des organisations, 6 édition, Vuibert, Paris, 2011, p : 5.

يوضح الشكل أعلاه مكونات نظام المعلومات وأهدافه، حيث يتفاعل كل من الأفراد،

الأجهزة، البرامج والمعطيات فيما بينها، من أجل جمع، معالجة، تخزين ونشر المعلومات.

ثانيا: أهداف نظام المعلومات

لنظام المعلومات مجموعة من الأهداف تتمثل في مايلي[2]:

- تحسين الفعالية: وهي عمل الأشياء بشكل صحيح؛

[1] هويدا علي عبدالقادر، **"نظم المعلومات الإدارية النظرية والتطبيق"**، دار الجنان للنشر والتوزيع، الخرطوم، 2011، ص: 29.

[2] محمد بن أحمد بن تركي السديري، **"نظم المعلومات الإدارية"**، جامعة الملك سعود، 2012، ص: 23.

- تحسين الكفاءة: وتعني عمل الأشياء الصحيحة فهي تعني عمل الأشياء التي أن نعملها ونحتاج إلى عملها لتحقيق نتائج جيدة و أهداف مرسومة؛
- سهولة التحول: لاشك أن استخدام نظم المعلومات والتقنية يعمل على تغيير طرق وأساليب القيام بالأعمال؛
- زيادة دقة المعلومات: لابد أن تقدم نظم المعلومات دقة عالية يمكن الاعتماد عليها؛
- تحسين جودة المنتج والإنتاجية: لابد أن يكون المنتج ذا جودة عالية ويطابق معايير الجودة؛
- تخفيض التكاليف: وذلك من خلال سرعة توفير المعلومات للتمكن من سرعة اتخاذ القرار الذي يقلل من كمية الهدر في المدخلات والمخرجات؛
- ربط العملاء بالشركة: من خلال ربط العملاء بالشركة بقواعد البيانات؛
- زيادة القيمة المضافة: وتقاس قيمة المعلومات بمدى تغطية المنفعة الناتجة عنها لتكلفة إعدادها؛
- تقليل وقت الحصول على المعلومات.

ثالثا: عناصر نظم 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:

1. **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 النظام[1].
2. **المعالجة:** تتم معالجة البيانات المدخلة بإجراء عدد من العمليات لإنتاج المخرجات المعينة المحتاج إليها[2].
3. **المخرجات:** تتحول المدخلات بفعل عمليات المعالجة إلى المخرجات التي تطرح في البيئة المحيطة أو تستخدم كمدخلات جديدة للنظام نفسه، والتي تكون على نوعين حصرا في جميع أنواع الأنظمة وهما المادة فقط أو المعلومات فقط أو كليهما معا.
4. **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.

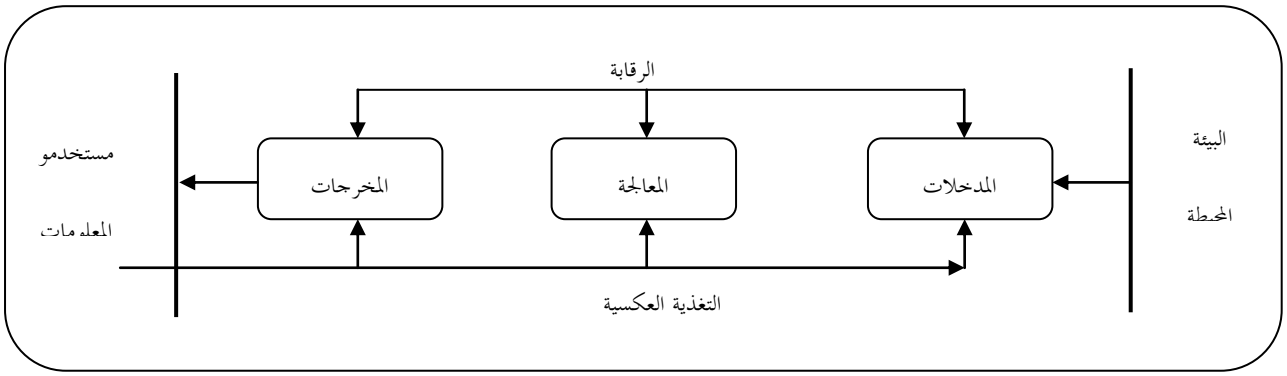
[1] محمد آل فرج الطائي، **"الموسوعة الكاملة في نظم المعلومات الإدارية الحاسوبية"** دار زهران، الأردن، 2002، ص: 44

[2] أبو بكر محمود الهوش ، **"نظم وشبكات المعلومات، مؤسسة الثقافة الجامعية"** مصر، 2007، ص:95

5. **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 متماشية مع الأهداف والخطط الموضوعة، فإذا كانت هناك أي انحرافات فإنه يجري القيام بالتعديلات اللازمة على المدخلات والعمليات والمعالجة وصولا لتصحيح المسار نحو الأهداف الموضوعة.
6. **البيئة:** تتأثر المؤسسة بالبيئة المحيطة بها، وتصدر مخرجاتها أيضا إلى هذه البيئة بعد تشغيلها، مما يعني وجود علاقة تبادلية وثيقة بين المؤسسة والبيئة المحيطة يؤثر كل منهما في الآخر سلبا أو إيجابا ويزداد هذا التأثير إذا كانت البيئة محكومة ومقيدة مثل النظم الاقتصادية والسياسية الموجهة أو المغلقة.

يوضح الشكل الموالي عناصر نظام المعلومات :

الشكل 1-2 : فعاليات نظام المعلومات



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

من خلال الشكل السابق، يتبين سير المعلومة بدءا من مستخدمي المعلومات ثم تحولها إلى مدخلة، ثم معالجتها ثم تحولها إلى مخرجات، كل هذا من خلال تواجد رقابة عبر كل المراحل.

رابعا: مكونات نظام المعلومات

يتشكل نظام المعلومات من مجموعة من المكونات التي يتم استخدامها للقيام باستقبال موارد البيانات وتحويلها إلى منتجات نهائية على شكل معلومات بداية من أنشطة الإدخال، التشغيل، المخرجات والرقابة، وتتمثل في[1]:

[1] جلال إبراهيم العبد، منال الكردي، **"مقدمة في نظام المعلومات الإدارية"**، دار الجامعة، الإسكندرية، 2003، ص 30

1. **الأجهزة والمعدات:** وتتضمن جميع الأجهزة المادية والمواد المستخدمة في تشغيل المعلومات وهي تشتمل على:
   - **نظم الحاسب :** تمثل وحدة التشغيل المركزية ووسائل التخزين الثانوية؛
   - **الأجهزة المكملة:** وتشتمل على الفأرة ولوحة المفاتيح والشاشة والطابعات؛
   - **الوسائط:** وهي جميع الأشياء الملموسة والتي يتم تسجيل البيانات عليها مثل الورق الأقراص الضوئية والممغنطة.

2. **البرمجيات:** وتشمل جميع أنواع تعليمات تشغيل البيانات وتتمثل في كل من:
   - برامج تشغيل النظام مثل برامج تشغيل العمليات، تدعيم القرارات والنظم الخبيرة؛
   - برامج التطبيقات؛
   - الإجراءات.

3. **العنصر البشري:** إن وجود الأفراد ضرورة لعمل أي نظام للمعلومات لأنه هو الذي يقوم بأنشطة تحليل وتخطيط البرامج والإشراف عليها وتوجيه النشاطات الفنية والإدارية المتعلقة بأفضل استغلال ممكن، وينقسم العنصر البشري إلى نوعين أساسين هما:
   - **المستخدمين النهائيين:** ويمثلون الأفراد الذين يستخدمون النظام بطريقة مباشرة أو من يستخدمون مخرجاته المجهزة بواسطة أطراف آخرين وأمثلة هؤلاء نجد المحاسبين، رجال البيع ، المهندسين، المدراء والعملاء؛
   - **الأخصائيون في النظام الآلي:** ويمثلون الأفراد الذين يطورون ويشغلون النظام ويشملون كل محللي النظام ومطوري البرامج ومشغلي النظام.

4. **قاعدة البيانات:** تدرك المنظمة في الوقت الحالي مدى أهمية البيانات التي تكسبها قيمة مضافة بعد تشغيلها لتصبح معلومة ضرورية ، كما أن إدارة هذه البيانات يؤدي إلى فعالية تفيد في النهاية جميع المستخدمين النهائيين داخل وخارج المنظمة.
5. **الشبكات:** أصبحت شبكات الاتصال مثل : الأنترانات والاكسترانات ضرورية في جميع أنواع المنظمات للقيام بالتجارة والأعمال الإلكترونية.

ونظم المعلومات وشبكات الاتصال تتكون من الحاسبات، مشغل الاتصالات وغيرها من الأجهزة المتصلة بوسائط الاتصال.

المطلب الثاني: مخاطر وتهديدات نظم المعلومات

هناك مجموعة من المخاطر والتهديدات التي تحيط بنظام المعلومات من شأنها أن تعيق السير الحسن لنشاطه وتختلف درجات تأثيرها بدرجة خطورتها والنتائج المترتبة عليها، ويمكن توضيحا في النقاط التالية[1]:

أولا : مخاطر نظم المعلومات

تصنف مخاطر نظم المعلومات إلى مجموعة من التصنيفات حيث يمكن تقسيمها إلى:

1. مخاطر من حيث المصدر:

أ .مخاطر داخلية: يعتبر موظفي المؤسسات، المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات، وذلك لأن الموظفين يكونون على علم ودراية بمعلومات النظام أكثر من غيرهم، إضافة إلى معرفة 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 المؤسسة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها.

ب .مخاطر خارجية: وتتمثل في أشخاص خارج المؤسسة ليس لهم علاقة مباشرة بها، مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عنها أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات، والتي قد تحدث تدمير جزئي أو كلي لنظام المؤسسة.

2. المخاطر من حيث المتسبب بها:

أ .مخاطر ناتجة عن العنصر البشري:وهي تلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل، السهو أو الخطأ.

ب .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.

[1]حرية شعبان الشريف، "**مخاطر نظم المعلومات المحاسبية الإلكترونية :دراسة تطبيقية على المصارف العاملة في قطاع غزة**"، مذكرة ماجستير غير منشورة، الجامعة الإسلامية غزة، 2006، ص:74.

3. المخاطر من حيث العمدية:

أ .مخاطر ناتجة عن تصرفات متعمدة: و تتمثل في تصرفات يقوم بها الشخص متعمدا مثل إدخال بيانات خاطئة وهو يعلم بذلك، أو قيامه بتدمير بعض البيانات متعمدا ذلك بهدف الغش، التلاعب أو السرقة، وتعتبر هذه المخاطر من أهم المخاطر المؤثرة على أمن النظام.

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

4. من حيث الآثار الناتجة عنها:

أ .مخاطر 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).

ب .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 للمؤسسة.

وقد تحدث المخاطر السابقة من خلال قيام المهاجم بالبحث في مخلفات التقنية الخاصة بالمؤسسة من قمامة وأوراق متروكة بهدف الحصول على أية معلومات قد تساعده 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.

5. المخاطر من حيث علاقتها بمراحل النظام:

أ .مخاطر المدخلات: وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال.

كما يمكن تقسيم المخاطر المتعلقة بأمن المدخلات إلى أربعة أقسام أساسية وهي:

- **إنشاء بيانات غير سليمة:** ويتم ذلك من خلال إنشاء 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 كشوف الرواتب وصرف رواتب شهرية لهم أو (إدخال فواتير وهمية باسم أحد الموردين)؛

- **تعديل أو تحريف بإنات 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 تغير أسماء بعض العملاء أو معدلات الفائدة.

- **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.

- **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 بإنات 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 .

ب .مخاطر معالجة البيانات: ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل 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، وتتمثل في:[1]

1-الوصول غير الشرعي للبيانات والنظام بواسطة الموظفين؛
2-الوصول غير الشرعي للبيانات والنظام بواسطة أشخاص من خارج المؤسسة؛
3-اشتراك العديد من الموظفين في نفس كلمة السر؛
4-إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام؛
5-اعتراض وصول البيانات من أجهزة الخادم إلى أجهزة المستخدمين.

[1]عصام محمد البحيصي و حرية شعبان الشريف، **"مخاطر نظم المعلومات المحاسبية الالكترونية"**، مجلة الجامعة الإسلامية، المجلد 16، العدد 2، غزة، 2008، ص ص: 904- 905

ج .مخاطر المخرجات: ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال:

1-طمس أو تدمير بنود معينة من المخرجات؛

2-خلق مخرجات زائفة /غير صحيحة؛

3-سرقة البيانات /المعلومات؛

4-عمل نسخ غير مصرح بها من المخرجات؛

5-الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق؛

6-طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك؛

7-المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخولين باستلام نسخة منها؛

8-تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.

ثانيا: تهديدات نظام المعلومات

ويقصد بعملية التهديدات هي أن هناك احتمال لعملية خرق أمني للمؤسسة أو الأفراد، وليس بالضرورة أن يكون الخرق قد حصل حقيقة ليتم اعتباره كتهديد[1].

هناك مجموعة من التهديدات التي يمكن أن يتعرض لها النظام وهي:

1. الوصول غير الشرعي للأجهزة والمعدات كالخوادم، الأجهزة الطرفية، أجهزة توزيع حركة الشبكة، يكون الهدف منه تدمير و إتلاف الأجهزة أو المعلومات، أو سرقة أو تعديل المعلومات، أو وضع أنظمة للتجسس و المراقبة[2].

ويكون هذا الوصول على شكل هجمات تأخذ مظاهر عدة منها:

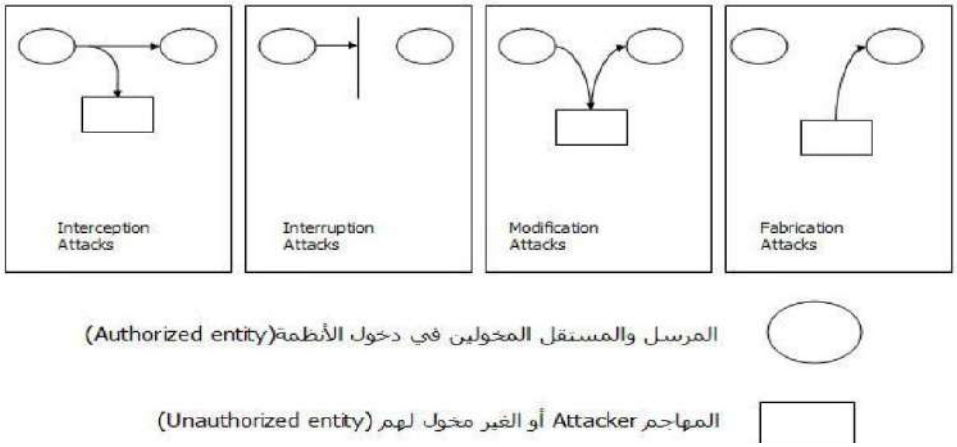
- ✓ هجوم التصنت على الرسائل: ويتم خلالها مراقبة الاتصال بين المرسل والمستقبل للحصول على المعلومات؛
- ✓ هجوم الإيقاف: ويعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل؛
- ✓ هجوم التعديل: وخلاله يتدخل المهاجم بين المرسل والمستقبل ويقوم بتغيير محتوى الرسالة؛
- ✓ الهجوم المزور أو المفبرك: وهنا ينتحل المهاجم صفة أحد الطرفين (المرسل أو المستقبل).

[1] خضر مصباح إسماعيل الطيطي، **"أساسيات أمن المعلومات والحاسوب"**، دار الحامد، الأردن 2010، ص39

[2] خالد رحم، ، **"محاضرات أمن نظم المعلومات"** مقياس مراجعة نظام المعلومات، أولى ماستر، جامعة ورقلة، 2015-2016

يوضح الشكل الموالي الأنواع الأربعة للهجمات :

الشكل : 1-3 : أنواع الهجمات



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

2. **البرمجيات الخبيثة:** وهي عبارة عن برامج تم إعدادها من قبل المبرمجين وذلك لغرض إلحاق الضرر بالبيانات المستهدفة كتخريبها و إزالتها أو السيطرة عليها وإلحاق الضرر بها، ويمكن أن تكون على شكل:

- ✓ فيروس: وهو عبارة عن كود برمجي الغرض منه إحداث أكبر قدر من الضرر، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى[1]؛
- ✓ الديدان: تصيب الحواسيب الموصلة بالشبكة بشكل أوتوماتيكي ومن غير تدخل الإنسان وهذا الأمر يجعلها تنتشر بشكل أوسع وأسرع عن الفيروسات، والفرق بينهم هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم بتهليك موارد الجهاز[2]؛
- ✓ حصان طروادة : وهو عبارة عن برنامج يغري المستخدم بأهميته أو بشكله أو بإسمه إن كان جذابا وفي الواقع هو برنامج يقوم بفتح باب إن صح التعبير بمجرد تشغيله، ومن خلال هذا الباب يقوم المخترق باختراق الجهاز وبإمكانه التحكم بالجهاز بشكل كبير[3]؛
- ✓ الباب الخلفي: وهي عبارة عن الثغرات الموجودة بقصد أو بغير قصد في أنظمة التشغيل[4].

[1] مروان العبد محمد أبو زعنونة و علاء الدين محمد الصويتي، **"مقدمة في أمن الشبكات"**، دار المعتز، الأردن، 2009، ص:.97

[2] نفسه، ص:96.

[3] نفسه، ص:96.

[4] خالد رجم، مرجع سبق ذكره.

المطلب الثالث: أمن نظم المعلومات

يناقش هذا المطلب أمن نظم المعلومات والسياسات الواجب تطبيقها داخل المؤسسة.

أولا: تعريف أمن المعلومات

التعريف الأول: عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضا لمخاطر الاختراق[1].

التعريف الثاني: هو مجموع الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر[2].

ثانيا: عناصر أمن المعلومات

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية أو الأدائية- وكذا هدف التدابير التشريعية في هذا الحقل ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها[3]:

- ✓ **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك؛
- ✓ **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح و لم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع؛
- ✓ **استمرارية توفر المعلومات أو الخدمة:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية و أن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها؛

[1] علي حسين أحمد الحمادي، **"أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية"**مذكرة ماجستير غير منشورة، جامعة الشرق الأوسط، الأردن، 2010، ص: 13.

[2] دلال صادق و حميد ناصر الفتال ،**" أمن المعلومات"**، دار اليازوري العلمية للنشر والتوزيع، الأردن ، 2008، ص ص: 11-12.

[3] موقع الانترنت : http://www.dralmarri.com/show.asp?field=res_a&id=205 يوم 2016/04/08 على الساعة : 20:05.

- ✓ **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به :** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات ، أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين[1].

ثالثا: مكونات أمن المعلومات

يمكن تقسيم مكونات أمن المعلومات إلى ما يلي[2]:

- ✓ أمن الأفراد والإدارة : وهي الإجراءات التي من شأنها الحفاظ على أمنية مركز الحاسبة وأخطار الأشخاص الغير مخولين من ذلك ، التحكم بدخول الأفراد، استعمال بطاقات هوية ممغنطة ، ... ألخ؛
- ✓ أمن المعلومات والوثائق في مراكز الحاسبات : إن الوثائق والحوامل الإلكترونية (أقراص، فلاش ديسك ... ألخ) ذات السرية العالية يجب حفظها في مواقع خاصة كما أن تصنيفها من حيث أهميتها وسريتها يعتبر من الوسائل المساعدة في هذه الوثائق؛
- ✓ أمن بناية مركز الخوادم: يدخل في هذا البند ، موقع مراكز الحاسبات والتصميم الهندسي لبناية هذه المراكز وكذا اختيار القاعة المخصصة لوضع الأجهزة ومتطلبات الحماية الأمنية لها ثم متطلبات الحماية و الأمن للمبنى ككل؛
- ✓ أمن الأجهزة البيئية الخاصة بمركز الخوادم: يعنى هذا البند بأمن أجهزة حفظ الطاقة و التبريد ووسائل الإطفاء الذاتي للحريق وكل ما له علاقة بالأجهزة البيئية؛
- ✓ أمن الاتصالات الخاصة بالحاسبات الإلكترونية : تعتبر الاتصالات في الوقت الراهن عصب الشبكات وحمايتها بالأولوية بمكان ويندرج في نطاق أمن الاتصالات، تأمين خطوط الاتصال وأجهزة الاتصال وحمايتها من الاختراق والتجسس.
- ✓ أمن أنظمة التشغيل والبرمجيات : تسعى المؤسسات لاتخاذ إجراءات واحتياطات أمنية لضمان سلامة أنظمة التشغيل والبرمجيات وجعلهما يمتلكا ن أساليب دفاعية ذاتية ضد محاولات التدخل غير المشروعة أو التخريب بكافة أشكاله، ومن بين الإجراءات المتخذة في هذا الجانب استعمال كلمات السر أو المرور، جدول الصلاحيات، التوثيق والنسخ الاحتياطي.

كما تعتبر الفيروسات بجميع أنواعها العدو اللدود لأنظمة التشغيل والبرمجيات المستعملة حيث يمكن أن يؤدي إلى تدمير البرامج، أو التجسس على البرامج، أو إحداث إعطاب على الأجهزة، لذلك وجب على المؤسسة أن تتوفر على برامج مضادات فيروسات، وكذا برامج برخص أصلية؛

[1] هويدا علي عبد القادر ، مصدر سابق، ص: 50.

[2] دلال صادق & حميد ناصر الفتال ،مصدر سابق، ص: 21.

- ✓ أمن أجهزة الحاسبات الإلكترونية: ويقصد بها الإجراءات المتخذة في تأمين الأجهزة الطرفية وملحقاتها المادية كالطابعات، وقارئ الأقراص المتعدد ... ألخ.

رابعا: تصميم نظام الحماية

لتصميم أي نظام أمني لحماية المعلومات يجب إتباع الخطوات التالية في تحديد المشاكل وإيجاد الحلول لها [1]:

- ✓ التهديدات الأمنية: يجب تحديد التهديد حتى يمكن تهيئة السلاح المضاد لمجابهته؛
- ✓ كلفة النظام الأمني: تلعب قيمة المعلومات دورا في تصميم النظام الأمني، فكلما كانت القيمة ثمينة كلما كان النظام الأمني معقد وثمين؛
- ✓ الوقاية : المقصود بها هو اتخاذ كافة الإجراءات والاحتياط اللازمة لمنع السرقة أو تدمير المعلومات . تعد الوقاية من أمثل المفاهيم النظرية ولكن يصعب تنفيذها عمليا.وتشمل الوقاية مفردات كثيرة تبدأ من نصب منظومات مكافحة الحريق ومولدات الكهرباء والأنظمة الكهربائية المستقرة وحافظات نسخ الملفات إلى نصب مراكز حواسيب كاملة لتكون البديل إلى المراكز المدمرة بالسبب الانفجار أو الحريق أو الكوارث الطبيعية ... ألخ؛
- ✓ الكشف: يجب أن تتوفر في النظام الأمني قابلية الكشف عن الانتهاكات وهو يعمل سوية في العادة مع الرقابة في النظام الأمني؛
- ✓ الردع : يجب توفير الردع المناسب للنشاطات التخريبية لأن ذلك يؤدي إلى خوف المخربين من اكتشاف أمرهم ومحاسبتهم؛
- ✓ تصحيح النظام: يجب اكتشاف نقاط الضعف في النظام الأمني وتصحيحيها بصورة مستمرة، انطلاقا من مبدأ عدم وجود نظام أمني مثالي دون أن تكون هناك نقاط ضعف يتسلل منها المتطفلون لذلك يجب فحص النظام الأمني عمليا لاكتشاف نقاط الضعف فيه حتى يمكن معالجتها؛
- ✓ الإبطال وإعادة البناء :عندما تفشل جميع الإجراءات الأمنية في التغلب على تهديد معين فإن الوسيلة الوحيدة الباقية هي إعادة تصميم النظام الأمني مرة أخرى مع اتخاذ الإجراءات الأمنية الجديدة التي تعمل على منع هذا التهديد.

المبحث الثاني: الأدبيات التطبيقية

[1] علاء حسين الحمامي، سعد عبد العزيز العاني ، **"تكنولوجيا أمنية المعلومات و أنظمة الحماية"**، وائل ، الأردن ، 2007، ص ص: 42-45.

سيتناول هذا المبحث الدراسات السابقة التي لها علاقة بموضوع الدراسة، باللغتين العربية والأجنبية ثم أوجه الشبه والإختلاف مع هذه الدراسة.

المطلب الأول :الدراسات السابقة باللغة العربية

سنتناول في هذا المطلب مجموعة من الدراسات باللغة العربية، لها علاقة بموضوع الدراسة.

أولا : دراسة سعد بن عبد الهادي بن جليغم (2014)[1]

جاءت هذه الدراسة تحت عنوان " تقويم الدور الرقابي لهيئة الاتصالات وتقنية المعلومات السعودية في الحد من المخاطر الأمنية لاستخدامات مواقع التواصل الاجتماعي"، وقد تبلورت مشكلة الدراسة في الإجابة على التساؤل الرئيسي التالي : كيف يتم تقويم الدور الرقابي لهيئة الاتصالات وتقنية المعلومات السعودية في الحد من المخاطر الأمنية لاستخدامات مواقع التواصل الاجتماعي؟، وقد تمثل مجتمع الدراسة في جميع العاملين بهيئة الاتصالات وتقنية المعلومات والبالغ عددهم 356 موظف، (هيئة الاتصالات وتقنية المعلومات السعودية) وتم اختيار العينة من العاملين بهيئة الاتصالات وتقنية المعلومات في حدودها الزمنية 2014، واتبع الباحث المنهج الوصفي التحليلي في دراسته، كما استخدم الاستبيان كأداة لجمع البيانات والمعلومات.

وقد توصل الباحث إلى مجموعة من النتائج كان أهمها، أن هناك نقص في العاملين المختصين في مجال أمن الحاسب الآلي والمعلومات، وتبين أن أغلب أفراد العينة كانوا إداريون، كما أن هناك نقص في التوعية بخصوص المخاطر الناجمة عن استعمال مواقع التواصل.

وفي النهاية أعطى الباحث مجموعة من التوصيات يمكن أن تساهم في التقليل من المخاطر، لعل أبرزها توفير الإمكانات البشرية والتقنية المتطورة للرقابة وإنشاء إدارة متخصصة في مكافحة الجرائم الإلكترونية.

ثانيا: دراسة غانم بن غزاي الروقي العتيبي (2013)[2]

[1] سعد بن عبد الهادي بن جليغم، **تقويم الدور الرقابي لهيئة الاتصالات وتقنية المعلومات السعودية في الحد من المخاطر الأمنية لاستخدامات مواقع التواصلالاجتماعي**، رسالة ماجستير في العلوم الإدارية غير منشورة، جامعة نايف العربية للعلوم الأمنية ، العربية السعودية، 2014.

[2] غانم بن غزاي الروقي العتيبي، **"أمن نظم المعلومات وعلاقته بمستويات الإبداع للعاملين في شركة الاتصالات السعودية بالرياض"**، رسالة ماجستير في العلوم الإدارية غير منشورة، جامعة نايف العربية للعلوم الأمنية، السعودية، 2013.

جاءت هذه الدراسة بعنوان "أمن نظم المعلومات وعلاقته بمستويات الإبداع للعاملين في شركة الاتصالات السعودية بالرياض"، وتلخصت مشكلة الدراسة في التعرف على العلاقة بين أمن نظم المعلومات ومستويات الإبداع للعاملين في شركة الاتصالات السعودية، خصوصا أن هناك من يرى أن أدوات وأساليب ممارسة أمن نظم المعلومات تشكل قيود على العاملين وتثبط فيهم روح الإبداع، وتمثل مجتمع الدراسة من العاملين في مبيعات كبار العملاء ومبيعات قطاع الأعمال في وحدة قطاع الأعمال بالشركة والبالغ عددهم 599 موظف بالسعودية، لعام 2013، وكان منهج الدراسة المتبع هو المنهج الوصفي.

وقد استخدم الباحث الاستبيان كأداة دراسة، وكانت أهم نتائجها أن أفراد العينة موافقون على واقع أمن نظم المعلومات كما يتوفر لديهم عناصر الإبداع وأكثرها عنصر المرونة، وكان هناك ارتباط طردي بين أمن نظم المعلومات ومستويات الإبداع لدى العاملين، كما خلصت الدراسة إلى عدم وجود فروق ذات دلالة إحصائية حول محور الإبداع باختلاف الوظيفة، بالمقابل هناك فروق ذات دلالة إحصائية حول محور أمن نظم المعلومات باختلاف الوظيفة وهي أكبر لدى الموظف.

ثالثا : دراسة فاطمة ناجي العبيدي (2012) [1]

وجاءت هذه الدراسة تحت عنوان "مخاطر استخدام نظم المعلومات المحاسبية المحوسبة وأثرها على فاعلية عملية التدقيق في الأردن"، وقد هدفت هذه الدراسة إلى التعرف على مخاطر استخدام نظم المعلومات المحاسبية المحوسبة وأثرها على فاعلية عملية التدقيق في الشركات المساهمة العامة المدرجة في بورصة عمان، وتكون مجتمع الدراسة من ثلاث فئات ذات صلة بالموضوع وهم (المديرون، المدققون الداخليون والخارجيون)، أما عينة الدراسة فبلغ عددها 203 فرد، تم اختيارهم من مجتمع الدراسة، لسنة 2012.

وقد توصلت الدراسة إلى عدة نتائج من أهمها ما يلي :

- وجود أثر ذي دلالة إحصائية للمخاطر البيئية الخاصة بنظم المعومات المحاسبية المحوسبة على فاعلية عملية التدقيق في الشركات المساهمة العامة الأردنية؛

- وجود أثر لمخاطر إدخال نظم المعلومات، تشغيل البيانات ومخرجات نظم المعلومات المحاسبية المحوسبة على فاعلية عملية التدقيق في الشركات المساهمة العامة الأردنية.

رابعا : دراسة حرية شعبان محمد الشريف (2006) [1]

[1] فاطمة ناجي العبيدي، **"مخاطر استخدام نظم المعلومات المحاسبية المحوسبة و أثرها على فاعلية عملية التدقيق في الأردن"** رسالة ماجستير في المحاسبة، جامعة الشرق الأوسط، الأردن، 2012.

تحت عنوان "مخاطر نظم المعلومات المحاسبية الإلكترونية" مع دراسة تطبيقية على المصارف العاملة في قطاع غزة، وقد حاولت هذه الدراسة التعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية والتعرف على أسباب حدوثها وإجراءات الحماية المتبعة لمواجهة تلك المخاطر، وكانت عينة الدراسة متكونة من جميع المصارف العاملة في قطاع غزة والبالغ عددها 12 مصرفا والتي تضم مدراء المصارف والمحاسبين ورؤساء الأقسام ومراجعو نظم المعلومات الإلكترونية والمراجعين الداخليين والمراقبين في تلك المصارف ومهندسو وموظفو دوائر تكنولوجيا أما الحدود الزمنية لها التي كانت سنة 2006 .

وقد توصلت هذه الدراسة إلى مجموعة من النتائج كان من أهمها هي اعتماد المصارف على النظام الآلي بشكل كبير مع قلة الموظفين المختصين في تكنولوجيا المعلومات في هذه المصارف، إضافة إلى أن الأنظمة المرتبطة مع شبكة الانترنت كانت أكثر عرضة للفيروسات من الأنظمة الأخرى، وكانت مخاطر الإدخال غير المتعمد واشتراط الموظفين في كلمة السر وتوجيه المعلومات إلى أشخاص غير مصرح بهم تكرر شهريا.

وقد خلصت الدراسة في الأخير إلى مجموعة من التوصيات لعل من أهمها أن الإدارة الجيدة وتطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية، و اتضح أيضا أن المصارف العاملة في قطاع غزة تتبع إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية.

المطلب الثاني: الدراسات السابقة الأجنبية

أولا دراسة "MWITA SIMION MAROA" (2015)[2]

كان عنوان هذه الدراسة "العوامل المؤثرة في فعالية أمن نظم المعلومات في جامعة نيروبي"، عالجت هذه الدراسة العوامل المؤثرة في أمن نظم المعلومات وأخذت كدراسة حالة جامعة نيروبي، بمحاولة قياس أثر السياسات الأمنية على الفعالية الأمنية المتبعة في جامعة نيروبي، وقد تمثل مجتمع الدراسة المستهدف جميع مستعملي نظام المعلومات في جميع الكليات والإدارات الملحقة بجامعة نيروبي لسنة 2015، واستعملت الدراسة المنهج الوصفي، كما استعمل الباحث أسلوب الاستبيان حيث تم توزيع استبيان 130، وتمكن من استرجاع 120 بمعدل 92 بالمئة.

[1] حرية شعبان محمد الشريف، مرجع سبق ذكره.

[2] MWITA SIMION MAROA, « **Factors affecting information systems security effectiveness in university of Nairobi »,**Thesis of Master of science degree in information systems, Kenya,2015.

وقد خلصت الدراسة إلى مجموعة من النتائج تمثلت في أن دعم الإدارة العليا والسياسات الأمنية لنظم المعلومات، وتدريب المستخدمين وزيادة الوعي، يؤثرون على فعالية أمن نظم المعلومات في جامعة نيروبي لكن بدرجات مختلفة، حيث يزداد تأثير العوامل الثلاثة الأخيرة بقوة مقارنة بعامل دعم الإدارة العليا.

ثانيا: دراسة "KELEMIE TEBKEW YIRDAW" (2013) [1]

وقد جاءت هذه الدراسة تحت عنوان: "إدارة أمن المعلومات في البنوك الصناعية في أثيوبيا "، وعالجت هذه الدراسة إشكالية واقع أمن نظم المعلومات في القطاع البنكي الإثيوبي في ظل التحديات والتهديدات المتأتية من خلال التطور الكبير في قطاع الاتصالات التي تعتبر الوسط الحيوي نشاط هذه البنوك، وكان مجتمع الدراسة مكون من 20 بنك خاص وعام في إثيوبيا، أما العينة فتكونت من 5 بنوك لسنة 2013، واستعمل الباحث 3 طرق لجمع المعلومات: الاستبيان، تحليل الوثائق والمقابلة، واستطرد الباحث في تحليل البيئة التكنولوجية والاجتماعية وقد حاول ربط ذلك بعلاقة الأمن بالمعاملات البنكية، ليخلص في الأخير إلى أن الأمن أصبح مكون أساسي في النظام البنكي، ووجد مدى اهتمام البنوك به، وأوصى أن يعمم هذا الاهتمام على القطاعات الأخرى غير البنكية.

ثالثا: دراسة "DOREEN MORAA NYAMONG" (2012) [2]:

كانت هذه الدراسة تحت عنوان "إدارة أمن نظم المعلومات"، وكانت دراسة الحالة في جامعات كينيا، وحاولت هذه الدراسة التعرف على واقع إدارة أمن نظم المعلومات داخل الجامعات الكينية في ظل التطور الحاصل في التكنولوجيات الحديثة وكذا تنوع مصادر التهديد والمخاطر المتربصة بنظم المعلومات، وكان مجتمع الدراسة مكون من الأفراد المسؤولين على أمن المعلومات في الجامعات الكينية في حدودها الزمنية لعام الدراسة وهو 2012، بمنهج تحليلي استكشافي، هذه الدراسة بينت الفروقات في إدارة أمن المعلومات بين مختلف الجامعات الكينية، وبينت النتائج أن الجامعات أمام تحدي كبير من أجل وضع نظام أمني في ظل واقع بيئي متسارع داخل الجامعات.

[1] KELEMIE TEBKEW YIRDAW, « **Information security management framework for banking industry in Ethiopia** », Thesis of Master degree of science in information science, Ethiopia, 2013.

[2] DOREEN MORAA NYAMONGO, « **Information systems security management a case of private chartered universities in Kenya** », Thesisof Master of Science in Information Technology at Strathmore University, Kenya,2012.

المطلب الثالث: مقارنة الدراسات السابقة بالدراسة الحالية

من خلال عرض الدراسات السابقة، تبين أن هناك أوجه تشابه وأوجه اختلاف في جوانب كثيرة، كان أهمها:

- من ناحية الموضوع، معظم الدراسات اشتركت في موضوع واحد وهو أمن نظم المعلومات مع اختلاف في قطاع التطبيق فبعضها اختار الجامعات وبعضها اختارت البنوك، وبعضها تخصص في مخاطر الشبكات الاجتماعية؛
- من ناحية الهدف: اشتركت معظم الدراسات في هدف واحد وهو تقييم أمن نظم المعلومات في قطاعات مختلفة، وتحديد ما هي المخاطر وما هي الإجراءات الواجب اتخاذها أو مدى فعالية الإجراءات المتخذة؛
- من ناحية العينة: كان مجتمع الدراسة هو مجموع العاملين على نظم المعلومات سواء كانوا مستغلين للنظام أو الموظفين الذين يوفرون الدعم، وكانت العينة مختارة من هذا المجتمع؛
- الحد الزماني: هناك تباين زماني بين الدراسات، حتى ولو لم يكن كبير، إلا أن معامل الزمن في عالم التكنولوجيا يعتبر مهم جدا، كون هذا القطاع يشهد تطور متسارع، يستوجب في كل مرة مراجعة طرق وأساليب أمن نظم المعلومات، وقد قمنا باختيار مؤسسة تنشط في قطاع التكنولوجيا حيث البيئة الخصبة لكل نشاط تكنولوجي.

خلاصة الفصل:

تطرقنا خلال هذا الفصل لمختلف المفاهيم المتعلقة بنظام المعلومات ومكوناته، وكذلك المخاطر التي تتهدد النظام عبر عدة تصنيفات كان أهمها المخاطر والتهديدات المتعلقة 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 أخر تم التطرق لمفهوم أمن المعلومات، وعناصره ومكوناته، وكيفية تصميم نظام الحماية، وفي الأدبيات التطبيقية تناولنا في المجمل سبع دراسات سابقة منها أربعة باللغة العربية وثلاثة باللغة الأجنبية رسمت 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 عالجت تقييم أمن نظام المعلومات في الحد من المخاطر في مؤسسة اتصالات الجزائر (المفوضية الجهوية بورقلة).

الفصل الثاني:

الدراسة الميدانية في مؤسسة اتصالات الجزائر

تمهيد :

بعد أن تناولنا الجانب النظري للموضوع من خلال دراسة مفاهيم نظم المعلومات، والتعرف على المخاطر والتهديدات، وعرض الإجراءات والسياسات الأمنية للحد من هذه المخاطر، وكذا الدراسات السابقة التي تعرضت لموضوع البحث، سنحاول في هذا الفصل إسقاط هذه المفاهيم النظرية على الجانب الميداني.

وحتى نتمكن من الإلمام أكثر بالجانب التطبيقي لهذا الموضوع قمنا بتقسيم هذا الفصل إلى مبحثين، تطرقنا في المبحث الأول إلى التعريف بمجتمع وعينة الدراسة وتحديد متغيراتها، وكذا طريقة جمع المعطيات اللازمة في بناء هذه الدراسة، ومن ثمة تحديد الأدوات المستخدمة .

أما في المبحث الثاني تم التطرق إلى عرض ومناقشة النتائج المتوصل إليها، مع تقديم التفسيرات لهذه النتائج، وفي الأخير اختبار الفرضيات المقدمة في أول هذه الدراسة.

المبحث الأول: الطريقة والأدوات المستخدمة

سنتطرق خلال هذا المبحث إلى جوانب الدراسة والمتمثلة في طريقة الدراسة وأدوات الدراسة، بما في ذلك مجتمع الدراسة وعينتها، وتحديد متغيرات الدراسة.

المطلب الأول: طريقة الدراسة

سوف نتعرف على طريقة الدراسة من خلال تحديد مجتمع وعينة الدراسة، وتحديد المتغيرات.

أولا: مجتمع وعينة الدراسة

1 - **مجتمع الدراسة:** تم اختيار مؤسسة اتصالات الجزائر – المفوضية الجهوية للاتصالات بورقلة- كونها رائدة في مجال الاتصالات وبالتالي تتضمن جميع الوسائل المتعلقة بنظام معلومات إلكتروني.

تعريف بالمؤسسة: أنشئت إتصالات الجزائر في إطار قانوني مؤسسة ذات أسهم تنشط في سوق شبكات وخدمات الاتصالات الإلكترونية، بموجب المرسوم رقم 2000-03 بتاريخ 05 أوت 2000 الذي تم بموجبه إعادة هيكلة قطاع البريد والاتصالات في الجزائر والذي أدى إلى فصل النشاطات البريدية والخدمات الاتصالات، ودخلت رسميا في الخدمة ابتداء من 1 جانفي 2003[1].

تعتبر اتصالات الجزائر القاطرة الرئيسية لقيادة إستراتيجية تكنولوجيات الإعلام والاتصال في الجزائر وهذا بفضل شبكاتها الممتدة على كامل التراب الوطني، حيث تمتلك المؤسسة أكثر من 47000 كلم من الألياف البصرية.

تنقسم إتصالات الجزائر تنظيميا إلى ثلاث مستويات:

- المديرية العامة : ومقرها بالمحمدية الجزائر العاصمة.
- المفوضيات الإقليمية : وعددها 13 مفوضية تتوزع على كامل التراب الوطني، حيث تضم كل مفوضية مجموعة من الولايات، تسهر على متابعتها ودعمها، هذه المفوضيات هي : الجزائر، البليدة، تيزي وزو، عنابة، قسنطينة، سطيف، باتنة، الشلف، وهران، تلمسان، الأغواط، بشار، ورقلة.
- المديريات العملية: وهي الوحدة العملاتية لجميع نشاطات المؤسسة وعددها 50 مديرية (48 ولاية، بالإضافة إلى مديريتين إضافيتين بالعاصمة، حيث تحتوي على العاصمة على 3 مديريات عملية).

[1] https://www.algerietelecom.dz/siteweb.php?p=at_histoire_realisations , 23/04/2016 à 22:04

2 - **عينة الدراسة:** تتشكل عينة الدراسة 100 فرد من العاملين على نظام المعلومات داخل المؤسسة، سواءا كانوا موظفي استغلال، أو موظفي دعم ينشطون على مستوى الإقليم التابع للمفوضية الجهوية للاتصالات بورقلة.

ثانيا :متغيرات الدراسة

سنحاول فيما يلي تحديد متغيرات الدراسة.

المتغير التابع: ويتمثل في مخاطر نظم المعلومات وهو متغير نوعي.

المتغير المستقل: ويتمثل في أمن نظم المعلومات وهو متغير نوعي كذلك.

المطلب الثاني: أدوات الدراسة

خلال هذا البحث تم الاعتماد على أدوات البحث التالية :

1 - **المقابلة:**

حيث كانت أول مقابلة مع مسؤولي الموارد البشرية للتعرف عن كثب على الهيكل التنظيمي للمؤسسة، ومختلف مصالحها، وكذا على التعداد البشري داخل نظام المعلومات، خلال هذه المقابلة تم التعرف على :

- الهيكل التنظمي؛
- التعداد البشري.

كما تمت المقابلة مع مسؤولين عن نظام المعلومات GAIA وكانت أسئلة المقابلة محصورة في :

- مكونات نظام المعلومات؛
- نظام حركة المعلومة داخل النظام؛
- المخاطر التي تتهدد نظام المعلومات؛
- الإجراءات الأمنية.

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

3 - **الاستبيان:** وتم استخدامه لأجل جمع البيانات والمعلومات، وتم توزيعه على عينة مكونة من 100 فرد، وتم استرجاع 90 إجابة وتم تقسيمه إلى جزئين :

الجزء الأول : يتكون من المعلومات الشخصية.

الجزء الثاني : يحتوي على مخاطر وأمن نظم المعلومات والذي قسم بدوره إلى محورين :

المحور الأول: يتعلق بمخاطر نظم المعلومات ويتكون من 3 أبعاد، كل بعد يحتوي على 4 أسئلة.

المحور الثاني :الإجراءات الأمنية : وتم تقسيمه إلى 4 أبعاد، كل بعد 4 أسئلة.

بما مجموعه 28 سؤال للجزء الثاني، يتم الإجابة عنها من خلال 3 خيارات " غير موافق"، "موافق بشكل متوسط"، و "موافق".

المبحث الثاني: تحليل ومناقشة نتائج الدراسة

سنتناول في هذا المبحث عرضا لنتائج الدراسة، بعدها سنتطرق إلى مناقشة هذه النتائج وتفسيرها، وصولا إلى اختبار الفرضيات.

المطلب الأول : عرض نتائج الدراسة

سنتطرق في هذا المطلب إلى عرض نتائج المقابلة والملاحظة والإستبيان.

أولا : عرض نتائج المقابلة والملاحظة

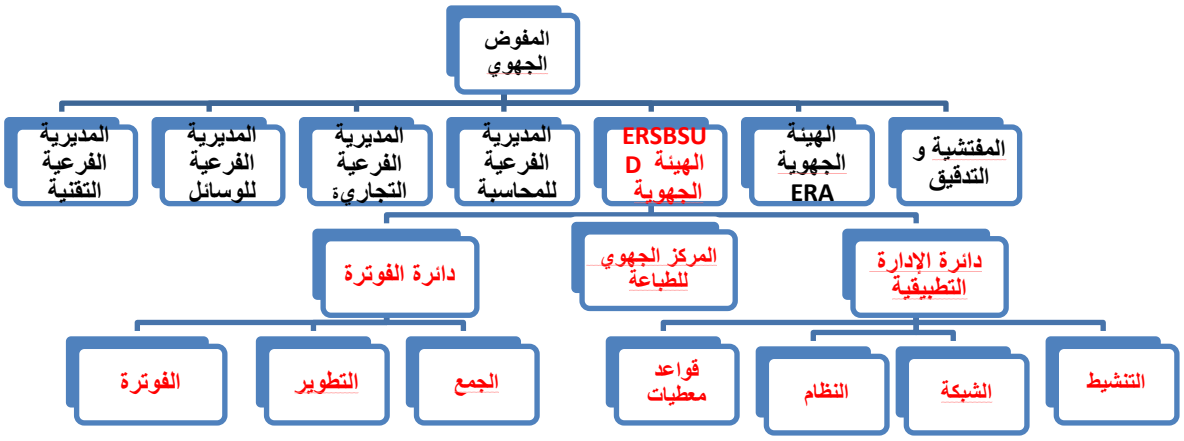
تمت الدراسة في المفوضية الجهوية لمؤسسة اتصالات الجزائر بورقلة على مستوى مجموعة من المصالح، التي تشترك في نظام المعلومات المستهدف بالدراسة.

وتضم هذه المصالح : مصالح التسيير التجاري، المصالح التقنية، مصالح الدعم، تتصل جميعها بمصلحة جهوية مكلفة بتسيير نظام المعلومات "قـــــايا"،وسنتطرق فيما يلي إلى الهيكل التنظيمي العام، وكذا وصف نظام المعلومات "قايا".

1 - الهيكل التنظيمي :

يبين الشكل التالي الهيكل التنظيمي للمفوضية الجهوية للإتصالات بورقلة

الشكل رقم 2-1 : الهيكل التنظيمي



المصدر : من إعداد الطالب بالاعتماد على معلومات مقدمة من طرف مصلحة الموارد البشرية

تتكون المفوضية الجهوية من أربعة مديريات فرعية (تقنية، وسائل عامة،تجارية ومحاسبة) كما تضم هيئتين، الهيئة الجهوية لأنظمة الفوترة وقواعد المعطيات، وهيئة شبكات الوصول، بالإضافة إلى المفتشية والتدقيق.

ونخص بالدراسة الهيئة الجهوية لأنظمة الفوترة وقواعد المعطيات ERSBSUD، كونها هي المسؤولة عن تسيير نظام المعلومات .

2 - تقديم هيئة ERSBSUD:

هي هيئة لها مدير خاص بها، مكلفة بتسيير نظام المعلومات "قايا"، تتبع لها ثمانية ولايات وهي: الأغواط، بسكرة، تمنراست، الجلفة، ورقلة، إليزي، الوادي وغرداية حيث أن كل الوكالات التجارية ومصالح الخطوط الهاتفية مربوطة بهذه الهيئة[1].

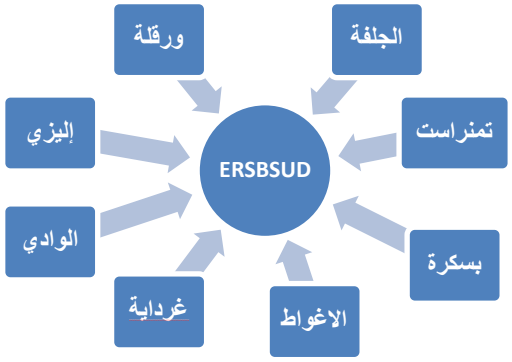
[1] بناءا على مقابلة مع السيد مدير ERSBSUD

وتضم هذه الهيئة ثلاث مصالح هي:

- دائرة الفوترة التي على مستواها يتم معالجة كل ما يتعلق بعملية الفوترة؛
- دائرة تسيير قاعدة المعطيات؛
- مركز الطباعة وهو المكلف بطباعة الفواتير وإرسالها للزبائن.

وفيما يلي تمثيل بياني للولايات المسيرة من طرف ERSBSUD :

الشكل رقم 2-2 : الولايات المسيرة من طرف ERSBSUD



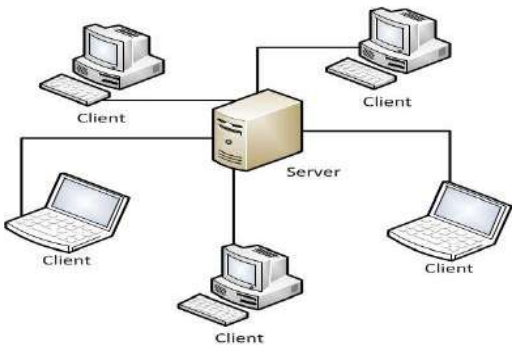
المصدر :من إعداد الطالب بالاعتماد على المقابلة مع السيد مدير هيئة ERSBSUD

نلاحظ بأن أغلب الولايات التابعة لهيئة ERSBUD تدخل ضمن الحيز الجغرافي للجنوب.

3 - وصف النظام :

بناءا على المقابلة والملاحظة تم تجميع المعلومات التالية : يتكون نظام معلومات من :الأجهزة والمعدات، البرمجيات، العنصر البشري، قاعدة البيانات والشبكات، ويعتمد على تقنية خادم/زبون كما هو مبين في الشكل التالي:

الشكل 2-3: تقنية خادم/زبون



Source : http://www.digitato.it/pro/windows-server/appunti-amministrazione-server-windows, 22/04/2016 à 22H00

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 ...ألخ.

I **الأجهزة والمعدات :** سيتم التركيز خلال هذه الدراسة على الخوادم، كون الزبائن لا يحتاجون لبيئة معقدة للعمل.

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 المكونات: يتكون النظام من مجموعة أجهزة مبينة في الجدول التالي :

الجدول رقم 2-1: مكونات نظام المعلومات

الرقم	البيان	العدد	الملاحظة
01	خادم : server، علامة BULL، ثماني النواة	05	تصل السعة التخزينة للخوادم 15 TB
02	الموجه : Router، علامة CISCO	02	
03	جدار ناري : Firewall، علامة stonesoft	02	
04	مولد كهربائي	01	
05	مخزن الطاقة KVA40	02	
06	مكيف هواء BTU50000	02	
07	مكيف هواء BTU18000	04	
08	نظام اكتشاف وإطفاء الحريق DEAI	01	
09	طابعة صناعية	01	
10	ربوت للتخزين الآلي في الحوامل الخارجية	01	

المصدر: من إعداد الطالب بالإعتماد على مقابلة مع السيد مدير ERSBSUD

يتضح من خلال الجدول أعلاه، أن أجهزة نظام المعلومات ذات نوعية وكفاءة عاليتين، وبكميات كافية.

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

أ -نظام التشغيل : تشتغل الخادمات 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 حتى الآن وهو في تطور مستمر.

يتكون هذا البرنامج من مجموعة من النماذج، تضمن التسيير الميسر للعمليات وسنتعرض الآن لمختلف الوحدات الموجودة :

الجدول 2-2 :نماذج نظام المعلومات "قايا"

النموذج	الشرح
نموذج العناوين	تسيير علاقات الزبائن CRM موجهة نحو الاتصالات
النموذج التجاري	تسيير الزبائن و إدارة المبيعات، تسيير كبار الزبائن grand comptes
نموذج المنتجات	شرائح المنتجات والخدمات
نموذج تسيير الاشتراكات	تقييم وحساب الاستهلاك
النموذج المالي	الفوترة، التحصيل، متابعة الديون، محاسبة
نموذج التعطلات	تسيير التعطلات
نموذج تسيير الشبكات	تسيير الحلقة المحلية للشبكة
نموذج الخرائط	مساعد جغرافي يسهل الوصول إلى معلومات الشبكة ويسمح بتسريع عملية
نموذج المعلومات	نظام مساعدة على اتخاذ القرار للمسيرين
نموذج مركز النداء	الوصول إلى المعلومات لمراكز النداء
نموذج البيانات	مستودعات البيانات
نموذج جمع البيانات	جمع البيانات
نموذج تنفيذ الأوامر	تأمين الاتصال بين النظام وأجهزة المحولات الهاتفية

المصدر: من إعداد الطالب بناء على المعطيات المقدمة من طرف المصلحة التجارية

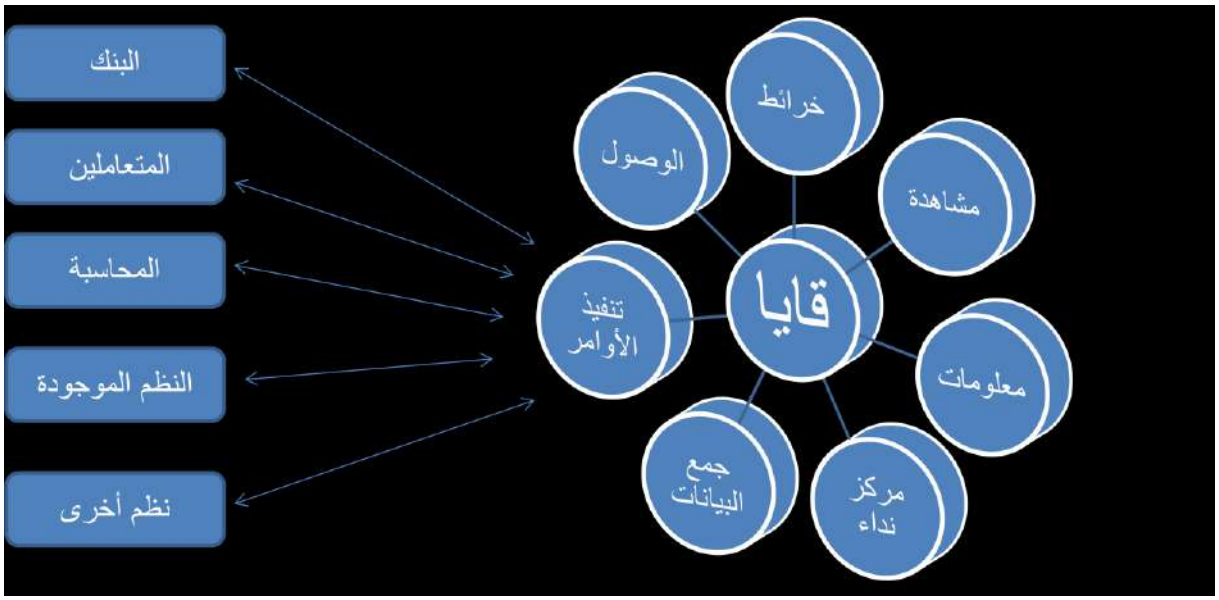
يتم إسناد إلى كل مستعمل لنظام المعلومات، نموذج أو أكثر للعمل عليها وإرفاقها بمجموعة من الصلاحيات.

ج –خصائص نظام المعلومات "قايا" :

– 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.

يبين الشكل التالي خصائص نظام المعلومات:

الشكل 2-4 :نموذج نظام المعلومات "قايا"



المصدر: المصلحة التجارية في مؤسسة إتصالات

من خلال الشكل المبين في الأعلى، تتضح قدرات نظام المعلومات "قايا"، حيث بإمكانه أن يتعامل مباشرة مع البنوك بواسطة واجهات خاصة، كما يمكن للمتعاملين أيضا الولوج لنظام المعلومات، كذلك الأمر لمصلحة المحاسبة، كما يمكنه التعامل كذلك مع أنظمة معلومات أخرى.

III – **التعداد البشري :** ينقسم العنصر البشري إلى شقين، الشق الأول وهم الأشخاص المسؤولين على تسيير نظام المعلومات، والشق الثاني يضم الأشخاص المستغلين لهذا النظام

-أشخاص الدعم : وهم التعداد المسؤول على صيانة وضمان السير الحسن لنظام المعلومات وعددهم 15 شخص موزعين حسب الجدول التالي:

الجدول 2-3 :توزيع موظفي دعم نظام المعلومات

الرقم	المؤهل	العدد	الملاحظة
01	ماجستير في الإعلام الألي	03	
02	مهندس دولة في الإلكترونيك	01	
03	مهندس دولة في الإعلام الألي	03	
04	ليسانس علوم تسيير	02	
05	تقني سامي في الإعلام الالي	03	
06	تقني سامي في الاتصالات	03	

المصدر : من إعداد الطالب بالاعتماد على مقابلة مع السيد مدير ERSBSUD

يتضح من خلال الجدول أعلاه، أن العنصر البشري الذي يسهر على سير نظام المعلومات ذو تكوين عالي في المجمل، حيث أن العمليات المعقدة يشرف عليها أفراد من حملة شهادة الماجستير في الإعلام الآلي بمساعدة المهندسين، أما العمليات ذات الجانب التجاري فيشرف عليها أفراد من حملة شهادة الليسانس في علوم التسيير، بمساعدة تقنيي الإعلام الآلي.

-الأشخاص المستغلون لنظام التشغيل: وهم جميع العمال في الوكالات التجارية والمصالح التقنية والإدارية.

IV - **قاعدة البيانات :** بنيت قواعد المعطيات لنظام المعلومات بقواعد المعطيات أوراكل وهو نظام قوي، كما يقبل لغة البرمجة الاستعلامية، التي تسمح بمحاورة قواعد المعطيات بسلاسة.

V - **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[1]: وهي شبكة عملاقة مكونة من مجموعة من الموجهات الكبيرة، والمجمعات، تتحكم في كامل الشبكة، تمر عبرها مختلف البيانات لمختلف الخدمات.

[1] RMS : Réseau Multi Services.

-شبكة LAN[1] : وهي شبكة محلية تستعمل البروتوكول TCP/IP قاعدة للاتصال، وتكون محدودة المكان.

-شبكة VPN[2] : وهي شبكة وهمية تستعمل الانترنت كقاعدة اتصال.

-شبكات X25 : شبكات قديمة تستخدم تقنية X25.

4 -**مستويات الوصول:** ويقصد بها الحدود المسموح بها لكل شخص الوصول إلى قواعد المعطيات والنظام ككل ويلخص الجدول التالي هاته المستويات حيث هناك نوعين من الوصول، وصول كامل يعني يصل إلى جميع الموارد ويستطيع أن يقوم بعمليات الحذف الإضافة، التعديل، ووصول جزئي أي يصل لجزء محدد فقط.

يبين الجدول الموالي مستويات الوصول حسب المستخدم:

الجدول 2-4 : مستويات الوصول

	مستخدم نهائي	الدعم	مدير قواعد المعطيات	المطور
المعطيات	**كامل**			
المتغيرات		**كامل**		**كامل**
القيم			**جزئي**	**كامل**
النظام		**جزئي**	**كامل**	**جزئي**

المصدر: من إعداد الطالب بالاعتماد على المقابلة مع مدير هيئة ERSBSUD.

من خلال الجدول السابق، يتبين أن المستخدم النهائي يتمتع بوصول كامل للمعطيات، كونه هو المسؤول عن إدخال المعطيات، أما أفراد الدعم فلهم وصول كامل للمتغيرات داخل النظام، ووصول جزئي لنظام في ذاته، أي يمكنهم فقد مشاهدة مكونات النظام، أما مدير قواعد المعطيات فهو الذي يملك الوصول الكامل للنظام كونه هو المسؤول عن إدارته وسيرورته، ويمكنه كذلك الإطلاع على القيم داخل النظام من غير القدرة على تغييرها، ويكون المطور (المبرمج) هو الذي يملك صلاحيات تغيير المتغيرات والقيم وله إطلاع على النظام من غير القدرة على تغييره، ولا يكون له وصول للمعطيات.

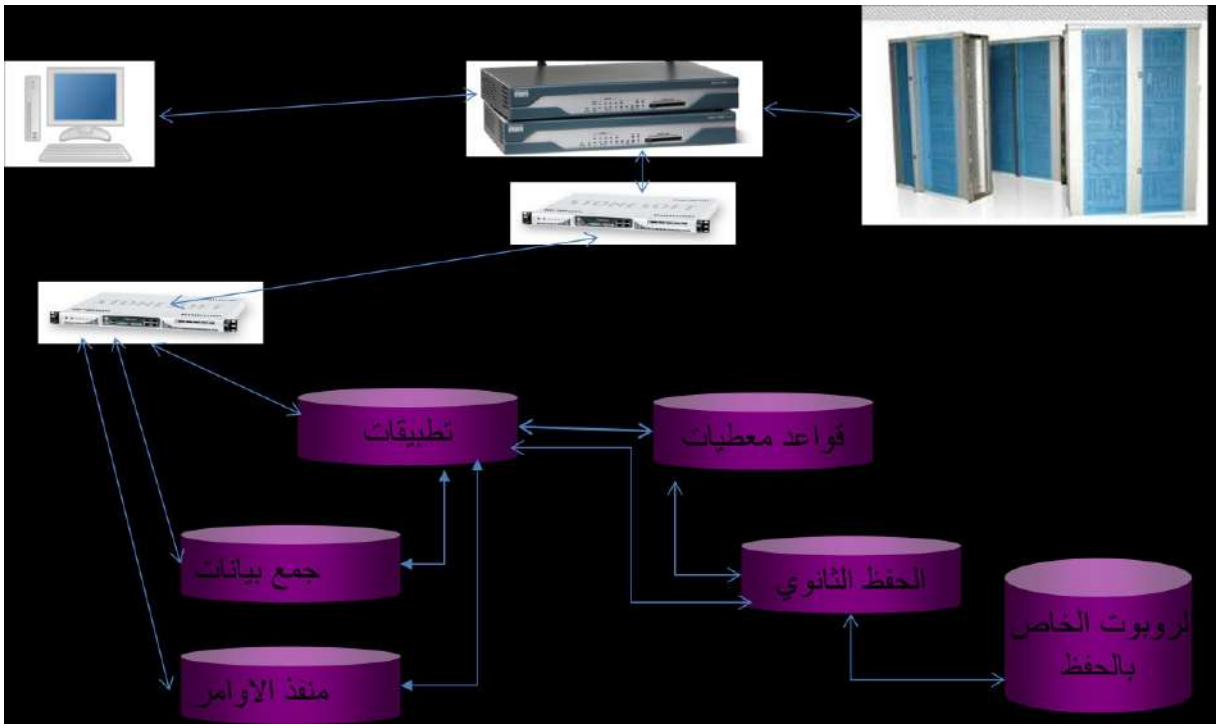
[1] LAN : Local Area Network.

[2] VPN : Virtual Private Network.

5 -سير الأوامر في نظام المعلومات :

يمثل الشكل التالي سير تنفيذ الأوامر في نظام المعلومات:

الشكل 2-5 : سيرورة الأوامر داخل نظام المعلومات"قايا"



المصدر : من إعداد الطالب بالاعتماد على المقابلة مع السيد مدير هيئة ERSBSUD

- ✓ يقوم المستخدم النهائي (الزبون) بمحاورة نظام المعلومات عن الطريق الشبكة المتوفرة لديه بواسطة محطة طرفية قد تكون حاسوب محمول أو حاسوب مكتب؛
- ✓ تنتقل البيانات بعدها إلى الموجهات؛
- ✓ قبل الوصول إلى الخادمات تمر عبر الجدار الناري الذي يقوم بدور الحماية؛
- ✓ تدخل البيانات إلى الخادم وتسجل في قواعد المعطيات؛
- ✓ ينشأ لكل أمر من نظام المعلومات، أمر موازي لأجهزة الاتصالات يتم تنفيذه عبر شبكة X25.

6 -السياسات الأمنية:

وتقسم السياسات الأمنية على عدة مستويات (الأفراد، المكان، الأجهزة و البرامج)، ويمكن شرحها بشكل مستفيض في العناصر التالية:

أ -السياسات الأمنية على مستوى الأفراد:

- 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 "قايا"، يحصل على كلمة سر واسم مستعمل خاص به و نموذج خاص به؛
- كل عملية تحدث على مستوى النظام تسجل باسم العامل الذي قام بها .

ب - السياسات الأمنية على مستوى المكان:

- موقع وجود خادمات 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.

ت - السياسات الأمنية على مستوى الأجهزة:

- 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، مخزنات الطاقة متوفرة وليست كافية؛
- شبكة محلية موجودة ترتبط بالخوادم عن طريق بروتوكلين TCP/IPو X25؛
- أجهزة اتصال، هاتف، فاكس متوفرة وتستعمل أحيانا؛
- الطابعات متوفرة سواء كانت مركزية أو شخصية.

ج- السياسات الأمنية على مستوى البرامج :وتنقسم إلى

ج.1- السياسات الأمنية على الخوادم

- برنامج تسيير قواعد البيانات عالي الأداء، وكذلك الحال لنظام التشغيل، البرنامج الرئيسي عبارة عن مجموعة مترابطة من الوحدات؛
- 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؛
- يعتبر الوصول إلى النظام عن طريق "تالنت" من أقوى نقاط قوة السياسيات 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.

ج.2- السياسات الأمنية على مستوى حواسيب الزبائن

- أنظمة التشغيل ويندوز من نسخ مختلفة منها الأصلية ومنها غير أصلية؛
- مضاد فيروسات مركزي مثبت في أغلب الحواسيب؛
- اتصال انترنت متوفر وبثلاث أشكال ويفي، شبكة، وأدي أس أل؛
- برامج متخلفة لأغراض متفرقة، عملية وشخصية؛
- الاتصال بنظام "قايلي" يتم على طريق بروتوكول "تلنت".

ثانيا : تحليل نتائج الإستبيان

تم توزيع 100 نسخة من الاستبيان، وتم استرجاع 90 نسخة أي 90% من النسخ الموزعة وكانت النتائج حسب برنامج SPSS كالتالي:

I **قياس ثبات وصدق أراء العينة (ألفاكرونباخ) :** يبين الجدول أدناه قيم معامل ألفاكرونباخ

الجدول 2-5 : جدول ألفاكرونباخ

	الأبعاد	التسمية	عدد الفقرات	قيمة ألفاكروميخ
المحور الأول	الأول	المدخلات	4	0.742
	الثاني	المعالجة	4	
	الثالث	المخرجات	4	
المحور الثاني	الأول	السرية أو الموثوقية	4	0.806
	الثاني	التكاملية وسلامة المحتوى	4	
	الثالث	استمرارية توفر المعلومات او الخدمة	4	
	الرابع	عدم الإنكار	4	
المجموع			28	0.772

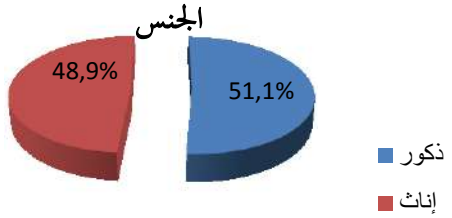
المصدر : من إعداد الطالب بالاعتماد على برنامج SPSS

تبين القيم المتحصل عليها على مدى صدق وثبات آراء العينة، حيث كانت مقبولة في المجمل بمعدل عام = 0.772، بمعنى أن الأشخاص المستجوبين لو أعيد استجوابهم تكون إجاباتهم في حدود 72 % من الاستجواب الأول، كما كانت نتائج المحور الثاني أكثر ثبات مقارنة مع نتائج المحور الأول.

II -توزيع العينة حسب المتغيرات الشخصية :

1-II حسب الجنس :

الشكل 2-6 :التوزيع حسب



ينقسم التوزيع حسب الجنس إلى :

إناث : 44 بنسبة 48.9%

ذكور : 46 بنسبة 51.1 %

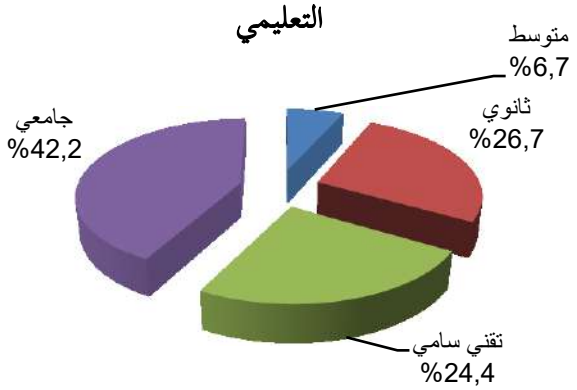
المصدر : من إعداد الطالب بالإعتماد على برنامج SPSS

وتبين النتائج أن العينة كانت متكافئة إلى حد بعيد من حيث التوزيع حسب الجنس.

II-2 حسب المستوى التعليمي:

كانت النتائج المتحصل عليها مايلي :

الشكل 2-7 :التوزيع حسب المستوى التعليمي



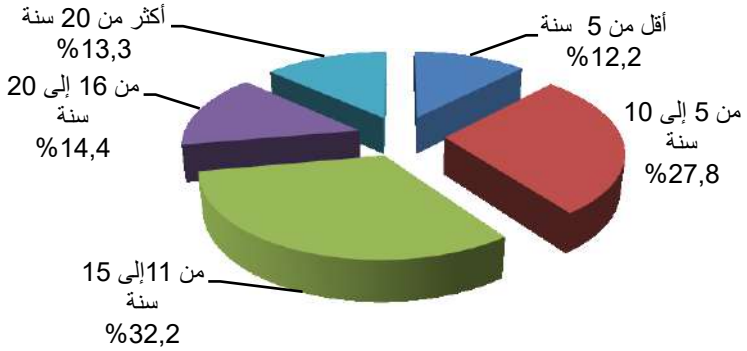
المصدر : من إعداد الطالب بالاعتماد على برنامج SPSS

تبين النتائج أن أغلب عناصر العينة كانوا من ذوي التكوين الجامعي، ثم جاء ذوو المستوى الثانوي يليهم أصحاب شهادات تقني سامي، أما أصحاب التكوين المتوسط فكانوا هم الأقلية.

II-3 حسب الخبرة :

كان توزيع العينة حسب الخبرة كمايلي :

الشكل 2-8 : التوزيع حسب الخبرة



المصدر : من إعداد الطالب بالاعتماد على برنامج SPSS

حيث أن أغلب عناصر العينة كانوا من ذوي الخبرة المتوسطة بين 11 إلى 15 سنة وهذا ما يفسره كون الشركة فتية، ثم تأتي بعدها العينة من ذوي الخبرة الحديثة نسبيا بين 5 إلى 10 سنوات، أما الفئات الأخرى فكانت متقاربة في نسبة تواجدها ضمن أفراد العينة.

II-4 نظام المعلومات في المؤسسة :

يبين الشكل الموالي أراء أفراد العينة حول نظام المعلومات داخل المؤسسة:

الشكل 2-9: نظام المعلومات

المصدر : من إعداد الطالب بالاعتماد على برنامج SPSS

وتبين العينة، أن أفرادها أكثر وعي كون نظام المعلومات يعتمد أكثر على الحاسوب، بالمقابل فئة قليلة قالت أن نظام المعلومات مشترك بين العمل اليدوي والعمل الآلي.

III - قياس اتجاه أفراد العينة نحو عبارات المحور الأول

الجدول 2-6 : مخاطر تهدد نظام المعلومات

	مخاطر تهدد نظم المعلومات	المقياس	غير موافق	متوسط	موافق	المتوسط المرجح	الانحراف المعياري	الاتجاه
1	هناك أخطاء غير متعمدة أثناء إدخال المعلومات	التكرار	17	47	26	2.10	0.688	متوسط
		النسبة	18.9	52.2	28.9			
2	يتعرض النظام الى ادخال بيانات خاطئة عمدا لاغراض معينة	التكرار	71	12	7	1.29	0.604	غير موافق
		النسبة	78.9	13.3	7.8			
3	يشترك الموظفون في المصلحة بكلمة سر واحدة	التكرار	60	16	14	1.49	0.753	غير موافق
		النسبة	66.7	17.8	15.6			

.../...

.../...

4	يستعمل الحوامل الخارجية فلاش ديسك لإدخال البيانات	التكرار	31	29	30	1.99	0.828	متوسط
		النسبة	34.4	32.2	33.3			
5	تعرض إلى هجمات فيروسية من داخل الشبكة	التكرار	23	50	17	1.93	0.667	متوسط
		النسبة	25.6	55.6	18.9			
6	تعرض إلى هجمات فيروسية من خلال شبكة الانترنت	التكرار	45	25	20	1.72	0.808	متوسط
		النسبة	50.0	27.8	22.2			
7	توقف(تعطل) النظام بسبب خلل في الشبكة	التكرار	17	43	30	2.14	0.712	متوسط
		النسبة	18.9	47.8	33.3			
8	توقف(تعطل) النظام بسبب خطأ في استعمال الأجهزة	التكرار	25	46	19	1.93	0.700	متوسط
		النسبة	27.8	51.1	21.1			
9	إنشاء مخرجات مزيفة مشابهة للأصل التي تستخرج بواسطة النظام	التكرار	57	26	7	1.44	0.638	غير موافق
		النسبة	63.3	28.9	7.8			
10	الوصول غير المرخص للبيانات من طرف الموظفين	التكرار	63	20	7	1.38	0.628	غير موافق
		النسبة	70.0	22.2	7.8			
11	الوصول غير مرخص للبيانات من طرف أفراد خارج المؤسسة	التكرار	70	13	7	1.30	0.608	غير موافق
		النسبة	77.8	14.4	7.8			
12	طمس أو تدمير بنود من المخرجات	التكرار	58	29	3	1.39	0.555	غير موافق
		النسبة	64.4	32.2	3.3			
الكلي						1.93	0.452	

المصدر: من إعداد الطالب بالاعتماد على برنامجSPSS

بتحليل نتائج الاستبيان تبين أن الإجابات كانت في اتجاه غير الموافق، وموافق بشكل متوسط، حيث لم يحظ أي سؤال بموافقة في اتجاهه العام. وكانت النتيجة كما يلي:

- أكبر مخطر يتهدد نظام المعلومات كان تعطله بسبب خلل في الشبكة وكانت الإجابة بموافق بشكل متوسط أي تحدث أحيانا وهي نتيجة مقبولة عموما لنظرا لكبر حجم الشبكة وتعقيدها.
- الأخطاء غير المتعمدة خلال عمليات الإدخال، كانت في المرتبة الثانية من حيث المخاطر ودائما بدرجة عدم اليقين وهي إجابة منطقية.
- استعمال الحوامل الخارجية كان في المرتبة الثالثة، وقد وجد أثناء إجراء البحث بعض الحواسيب التي تم التعطيل العمدي لمنافذ الحوامل الخارجية لكي لا تستعمل، من أجل توفير حماية أكبر، إلا أن هذا الإجراء محدود وغير معمم على كامل الحواسيب المكونة للنظام.

- الهجمات الفيروسية داخل الشبكة، وتعطل الأجهزة كانا في مرتبة واحد من حيث قيمة المتوسط، في فيما يخص الهجمات الفيروسية يبين أن الحركة داخل الشبكة نشطة.
- أما الهجمات المتأتية من شبكة الانترنت ويرجع ذلك إلى استعمال الحواسيب للعمل على النظام والإبحار في الانترنت في نفس الوقت.
- باقي الأسئلة كان اتجاهها العام بغير موافق، من تلك الأسئلة كانت الإجابة عن سؤال اشتراك أكثر من شخص في كلمة المرور بغير موافق، وهذا ما لمسنا عكسه خلال محاورتنا لبعض العمال، حيث أكدوا أنهم أحيانا كثيرة يستعملون حسابات زملائهم من أجل الدخول إلى النظام، وهذي ثغرة كبيرة على نظام المعلومات.

IV - قياس اتجاه أفراد العينة نحو عبارات المحور الثاني

الجدول 2-7 : السياسات الأمنية

	السياسات الأمنية المتبعة	المقياس	غير موافق	متوسط	موافق	المتوسط المرجح	الانحراف المعياري	الاتجاه
1	يتم إدخال المعلومات بعد مصادقة المسئول المباشر	التكرار	9	32	49	2.44	0.672	موافق
		النسبة	10	35.6	54.6			
2	يتم تحسيس الموظفين بمخاطر نظم المعلومات	التكرار	19	29	42	2.26	0.787	متوسط
		النسبة	21.1	32.2	46.7			
3	يتم تكوين العمال عند تحديث النظام	التكرار	4	24	62	2.64	0.567	موافق
		النسبة	4.4	26.7	68.9			
4	المكان المخصص لأجهزة ربط الشبكة مؤمن ولا يسمح لغير المختصين بالوصول إليه	التكرار	15	22	53	2.42	0.764	موافق
		النسبة	16.7	24.4	58.9			
5	يتم تثبيت مضادات الفيروسات والتحديثات المتعلقة بها	التكرار	24	33	33	2.10	0.794	متوسط
		النسبة	26.7	36.7	36.7			
6	يتم منع الدخول لمواقع انترنت محددة بطريقة مركزية	التكرار	16	20	54	2.42	0.779	موافق
		النسبة	17.8	22.2	60			

.../...

.../...

7	تحتوي الشبكة على جدار ناري يمنع التسلل عبرها	التكرار	8	31	51	2.48	0.657	موافق
		النسبة	8.9	34.4	56.7			
8	لا يسمح بتثبيت البرامج المقرصنة وغير المرخصة	التكرار	13	30	47	2.38	0.728	موافق
		النسبة	14.4	33.3	52.2			
9	يتم صيانة الشبكة دوريا	التكرار	18	40	32	2.16	0.733	متوسط
		النسبة	20	44.4	35.6			
10	يتم عمل نسخ احتياطي ة للبيانات	التكرار	5	35	50	2.50	0.604	موافق
		النسبة	5.6	38.9	55.6			
11	يتدخل المختصين بكفاءة لإصلاح أي عطل	التكرار	9	37	44	2.39	0.665	موافق
		النسبة	10	41.1	48.9			
12	يتم تغيير الأجهزة دوريا لتوافق أخر التطورات التكنولوجيات	التكرار	11	42	37	2.29	0.665	متوسط
		النسبة	12.2	46.7	41.1			
13	يتم تغيير كلمة المرور دوريا	التكرار	15	44	31	2.18	0.674	متوسط
		النسبة	16.7	48.9	34.4			
14	يتم التصريح بعناوين الحواسيب (IP) حتى يتم الدخول للنظام	التكرار	8	17	65	2.63	0.644	موافق
		النسبة	8.9	18.9	72.2			
15	تسجل أي عملية أثناء المعالجة بإسم المستخدم الذي قام بها	التكرار	3	16	71	2.76	0.504	موافق
		النسبة	3.3	17.8	78.9			
16	الحواسيب محمية بكلمات مرور شخصية	التكرار	11	35	44	2.37	0.694	موافق
		النسبة	12.2	38.9	48.9			
المجموع						2.35	0.537	

المصدر : من إعداد الطالب بالاعتماد على برنامج SPSS

من خلال الجدول أعلاه يتضح أن المتوسط الحسابي الإجمالي للعينة = 2.35 أي أن المستجوبين يتفقون على أن هناك سياسة أمنية متبعة في المؤسسة، حيث أن:

- كان السؤال 15 أكبر العبارات موافقة من طرف العينة، هذا السؤال متعلق بتسجيل العمليات على النظام باسم صاحبها، وهي إجابة مقبولة جدا، إذ أن الموظف العامل على نظام المعلومات، يمكنه بسهولة تتبع من قام بالعمليات أثناء عمليه إبحاره داخل النظام، فهي ظاهرة للعيان.
- أما بالنسبة للسؤال الثالث المتعلق بالتكوين بعد تحديث النظام فكانت رتبة الإجابة الثانية في مجمل الإجابات وهي نتيجة مقبولة جدا وملموسة كذالك كما في الأولى، حيث أن عملية التكوين ظاهرة أمام العيان ويستفيد منها تقريبا كل موظف يعمل على النظام.
- في الرتبة الثالثة من حيث الإجابات كان السؤال 14 المتعلق بالتصريح ب عنوان IP كانت الأكثر موافقة، وهي إجابة مقبولة جدا، وملموسة في آن، ذلك أن حتى لو حاول الموظف الدخول للنظام أمام حاسوب غير مصرح العنوان، سيمنع أليا، وتظهر أمامه رسالة خطأ مفادها أنه يجب عليه أن يصرح أولا بالعنوان.
- كان السؤال العاشر موجه حول النسخ الاحتياطي وأجمعت العينة على أنه يوجد هناك نسخ احتياطي، وهو إجراء مهم للمؤسسة، إذا الإجابة كانت مقبولة.
- أغلب المستجوبين أكدوا على وجود جدار ناري بالمؤسسة، وهو يعكس مدى إلمام العمال بمكونات النظام، كون أن الجدار الناري غير محسوس الأثر وكونه يوجد في مكان تواجد النظام.
- أجمع المستجوبون أنه يتم إدخال المعلومات بعد مصادقة المسؤول المباشر، وهي إجابة مقبولة، وتسمح المشاركة في تحمل المسؤولية.
- أغلب أعضاء العينة قالوا بأن المكان المخصص للأجهزة مؤمن، وهي إجابة مقبولة عموما، لكن ما تم ملاحظته أثناء إعداد هذا البحث أن هذا المكان كان يمكن أن يكون أكثر تأمينا إذا تم الاعتماد على استخدام الدخول الإلكتروني باستعمال البطاقات الممغنطة.
- السؤال المتعلق بالدخول المشروط لمواقع الانترنت كان متوسطه = 2.42 وهي إجابة مقبولة، حيت يتم منع الدخول إلى بعض المواقع الإلكترونية.
- وافق أغلب أعضاء العينة على أنه يتم التدخل لإصلاح الشبكة بكفاءة وكانت قيمة المتوسط=2.39.
- السؤال المتعلق بتثبيت البرامج الأصلية، أفصح أغلب أفراد العينة على أنه يمنع تثبيت البرامج غير الأصلية.
- وقال أغلب أفراد العينة أن الحواسيب محمية بكلمات مرور، وهي نتيجة مقبولة.
- تردد أفراد العينة في السؤال المتعلق بتغيير الحواسيب بشكل دوري، وهو ما لوحظ خلال إجراء البحث من وجود بعض الحواسيب القديمة، والتي ما زالت تستعمل.
- تردد كذلك المستجوبون حول التخسيس بمخاطر الاختراق ومخاطر نظم المعلومات بصفة عامة، وهذا ما لمسناه من عدم وجود نشريات أو أوامر مصلحة تحذر من هذه الأعمال.

- التردد كان ملحوظ أيضا حول سؤال التغيير الدوري لكلمة المرور وهو إجراء أساسي لحماية نظام المعلومات، ومن خلال سؤالنا لبعض العمال حول تغيير كلمة المرور، أفصحوا بأنهم لم يغيروا كلمات المرور الخاصة بهم منذ أن استلموها للمرة الأولى.
- كذلك لم يكن الأفراد متأكدين من الصيانة الدورية للشبكة، وقد لوحظ أن المصلحة المختصة في صيانة الشبكة لا تتدخل عادة إلا في حالة وجود مشكل.
- وفي إجابة غريبة تردد الموظفون حول تثبيت مضادات الفيروسات والتحديثات الخاصة بها، مع أننا لمسنا وجود مضاد فيروسي مركزي ويقوم بالتحديث الآلي كل ما كانت هناك تحديثات متوفرة.

المطلب الثاني: مناقشة النتائج

خلال هذا المطلب سنقوم باستعراض نقاط القوة ونقاط الضعف لنظام المعلومات محل الدراسة، وكذلك سنقوم باختبار الفرضيات.

أولا: نقاط القوة والضعف

من خلال تحليل نتائج المقابلة، الملاحظة والاستبيان تمكنا من تحديد جملة من نقاط القوة ونقاط الضعف للنظام محل الدراسة.

1. نقاط القوة:

- يتميز النظام بسرعة تنفيذ المهام؛
- يتميز كذلك بسهولة مراقبة سيرورة العمل؛
- هو نظام مساعد على اتخاذ القرار، من خلال تزويد المسؤولين بكل المعلومات الضرورية وفي والوقت المناسب ومن خلال جملة الاستعلامات الملحقة بالنظام؛
- يعتبر وسيط بين أجهزة الاتصالات والموظفين بوصول سريع وآمن للأجهزة؛
- متوافق مع جميع تكنولوجيات الاتصالات، لمختلف الشركات أي إذا قررت المؤسسة تغيير أجهزة الاتصالات أو التكنولوجيا ككل فالنظام مجهز لذلك.

2. نقاط الضعف:

- لا توجد مذكرات مصلحية تحث على الأمن أو إجراءاته، وهذه من أكبر العيوب، ولمحنا ذلك من خلال الملاحظة وكذا المقابلة وتم إثبات ذلك من خلال الاستبيان؛

- في حالة انقطاع الخدمة، تبقى التعليمات عالقة مما يستدعي تدخل نصف آلي للأوامر من خلال مركز وسيط مخصص لهذا الغرض؛
- نسخ البرامج في بعض حواسيب العمال ليست أصلية مما يعرض الحواسيب للتعطل في حال تمت ترقية البرامج؛
- شبكة الويفي، يمكن أن تشكل ثغرة لاختراق النظام من خلال دخول أشخاص غرباء لشبكة المؤسسة؛
- شبكة X25 ثقيلة نوعا ما مقارنة بشبكة IP، مما يستدعي ترقيتها؛
- عدم وجود اتصال بين الطابعة المركزية والنظام مع تكرار تعطلاتها؛
- في حالة الطباعة يتم تحويل الملفات بواسطة فلاش ديسك مما يعرض المعلومات للضياع والفيروسات؛
- انعدام التكوين و الكفاءة في صيانة آلات الطباعة مما يؤدي إلى إرسالها إلى المديرية المركزية في حالة تعطيلها من أجل الصيانة أو جلب تقنيين من المديرية العامة.

ثانيا: اختبار الفرضيات

الفرضية الأولى : تنص هذه الفرضية على **"تتعدد المخاطر التي تهدد نظام المعلومات بحسب مراحل النظام في حد ذاته، فهناك مخاطر متعلقة بعمليات الإدخال، ومخاطر متعلقة بعملية المعالجة، ومخاطر متعلقة بالمخرجات".**

من خلال ما تم ملاحظته، وجمعه خلال المقابلة والاستبيان، تبين أن هناك مخاطر حسب مراحل النظام، لكن من خلال تحليل الاستبيان تبين أن العينة تعتقد بوجود مخاطر مدخلات و معالجة بدرجة مترددة، لكن لا تعتقد بوجود مخاطر حول المخرجات، ومن خلال الجدول رقم (2-6) فقد كان المتوسط الحسابي للعينة الذين أقروا بوجود مخاطر المدخلات = 1.72، أما المعالجة فكان المتوسط= 1.93، وفي النهاية المتوسط الخاص بالمخرجات = 1.38، ويرجع ذلك إلى عدم وجود حملات تحسيسية حول مخاطر المحدقة بنظام المعلومات، وهذا ما تجلى من خلال عدم وجود إرساليات مصلحية، ويلاحظ ذلك كذلك حين الرجوع للسؤال الثاني في محور الأمن فقد كانت إجابة العينة مترددة حول وجود تحسيس بمخاطر أمن المعلومات، **ومنه تم قبول هذه الفرضية.**

الفرضية الثانية: " تسمح السياسات الأمنية بزيادة أداء المكونات المادية والبرمجية وديمومة عمل نظام المعلومات لنظم المعلومات "

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 الأمنية المطبقة على حماية البرامج، من وجود نظام تشغيل UNIX، ومضادات الفيروسات والوصول بواسطة بروتوكول "تلنت"، كل هذه الإجراءات أكدت وحسب تصريح مدير هيئة ERSBSUD، 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 بمكوناته المادية والبرمجية، **وبالتالي قبول هذه الفرضية.**

الفرضية الثالثة: "يتمتع الأفراد العاملون على نظم المعلومات بدرجة وعي أكبر للمخاطر في حال العمل في بيئة ذات سياسات أمنية عالية"

بالرجوع إلى نتائج الاستبيان يتبين أن هناك إجراءات أمنية مستوعبة من طرف الأفراد العاملين على نظام المعلومات، بالمقابل تنخفض درجة الاستيعاب بالمخاطر المحدقة بنظم المعلومات، 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 ناحية المخاطر في حال العمل في بيئة ذات سياسات أمنية عالية وقد يعود ذلك إلى التقصير في إعلام هؤلاء الأفراد بواسطة التعليمات والمنشورات، **ومنه فإننا نرفض الفرضية الثالثة.**

خلاصة الفصل:

كان هذا الفصل عبارة دراسة تطبيقية لإسقاط ما تم التطرق إليه في فصل الأدبيات النظرية، وذلك من خلال دراسة حالة مؤسسة اتصالات الجزائر، واختبار الفرضيات الموضوعة سالفا.

فقد قمنا باستعراض متغيرات الدراسة ومجتمعها، وطرق جمع البيانات، كما استعرضنا تقديم للمؤسسة محل الدراسة، والمصلحة المسؤولة عن نظام المعلومات، وتم كذلك عرض النتائج وتحليلها ومن ثمة اختبار فرضيات الدراسة.

وكانت 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 عمليات تحسيسية من خلال المنشورات والتعليمات التي تبين مخاطر نظم المعلومات وتحث على تطبيق السياسات الأمنية، لأن هذا قد يؤدي إلى عدم استيعاب الأفراد للمخاطر المحيطة بنظم المعلومات، ومن ثم سيؤدي ذلك إلى حدوث مخاطر على مستوى النظام ككل.

الخاتمة

الخاتمة:

تستند الشركات الكبرى على أنظمة معلومات قوية، ومهيكلة بطريقة جيدة، لكي تتمكن من مواجهة كم المعلومات الهائل لعملائها، حيث تم ثل هذه الأنظمة دورا محوريا لاستمرارية نشاط ه ذه الشركات، حيث كلما كان نظام المعلومات أكثر تكامل، كلما كانت النتائج المرجوة أقرب إلى التحقيق داخل المنظمة أو الشركة.

ويبقى نظام المعلومات داخل مؤسسة اتصالات الجزائر دون التطلعات المرجوة، بالرغم من كل الايجابيات التي يحتويها، كون هذه المؤسسة هي رائدة الاتصالات في الوطن، فالأحرى بها أن تعكس هذه الريادة داخل كيانها.

نتائج البحث:

- ✓ توجد مجموعة من المخاطر تحيط بنظام المعلومات، وجب على موظفي دعم نظام المعلومات تحسيس الموظفين بهذه المخاطر؛
- ✓ تساهم السياسات الأمنية في التقليل من المخاطر المتعلقة بالمكونات المادية والبرمجية لنظم المعلومات؛
- ✓ عندما تكون الإجراءات الأمنية، يقل شعور الموظفين بالمخاطر المحيطة بنظام المعلومات .

التوصيات:

- ✓ تعريف وتحسيس المستخدمين الإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات وذلك بإصدار مذكرات مصلحيه، وتوجيهات بخصوص أمن نظم المعلومات؛
- ✓ استقطاب موظفي الدعم المختصين داخليين وخارجيين في أمن المعلومات للإشراف على هذا الجانب؛
- ✓ الاستغلال الأمثل لموارد النظام، لأن تجاهل إجراءات والتركيز على أخرى يمثل هدر لموارد المؤسسة بما يمثل استثمارات غير مستغلة؛
- ✓ ضرورة امتلاك الإدارة العليا لإستراتجية واضحة لأمن نظم المعلومات داخل المؤسسة؛
- ✓ تكوين العمال وتقديم نظرة شاملة على نظام المعلومات المستخدم داخل المؤسسة؛
- ✓ الاستغلال الأمثل للبرامج الموجودة من خلال تكوين العمال؛
- ✓ ضرورة مراقبة عملية الصيانة للأجهزة والبرامج، على أن تكون هذه العملية دورية ومنتظمة؛

- ✓ منع استعمال "الويفي" بالحواسيب المتصلة بنظام المعلومات، مع استعمال عقلاني للحواسيب المتصلة بالانترنت والانترانت؛
- ✓ تطوير الشبكة في ظل الإمكانيات المتاحة، لأنها تعتبر القاعدة الأساسية لنظام المعلومات؛
- ✓ تثمين السياسات الأمنية الخاصة بالخوادم، حيث لم تشهد هذه الأخيرة أي انقطاع لها منذ بداية دخولها للخدمة، لأن هذا الإجراء من شأنه تحفيز المكلفين بالعمليات الأخرى داخل المؤسسة.

أفاق الدراسة:

لقد سمحت هذه الدراسة الولوج إلى مواضيع أخرى يمكن أن تكون محاور بحث مستقبلية، حيث أن الخوض في موضوع أمن ومخاطر نظم المعلومات في بيئة تكنولوجية متجددة، تجعل من الصعب الوقوف عند حد معين، فيمكن البحث في مواضيع مثل:

- ✓ علاقة أمن المعلومات بأنظمة التشغيل داخل المؤسسة؛
- ✓ واقع تدقيق أمن نظم المعلومات في ظل معايير الجودة المطبقة في هذا المجال؛
- ✓ دور أمن نظم المعلومات في الحد من المخاطر، دراسة مقارنة بين مؤسسة خدمية وصناعية.

المراجع

أولا : المراجع باللغة العربية

I. الكتب:

1. أبو بكر محمود الهوش ، **"نظم وشبكات المعلومات، مؤسسة الثقافة الجامعية"**، مصر، 2007.
2. جلال إبراهيم العبد، منال الكردي، **"مقدمة في نظام المعلومات الإدارية"**، دار الجامعة ، الإسكندرية، 2003.
3. خضر مصباح إسماعيل الطيطي، **"أساسيات أمن المعلومات والحاسوب "**، دار الحامد، الأردن 2010.
4. دلال صادق و حميد ناصر الفتال ، **" أمن المعلومات"**، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2008.
5. عبد الرزاق محمد قاسم، **"تحليل وتصميم نظم المعلومات المحاسبية"**، دار الثقافة، دمشق، 2009.
6. علاء حسين الحمامي، سعد عبد العزيز العاني ، **"تكنولوجيا أمنية المعلومات و أنظمة الحماية"**، دار وائل، الأردن، 2007.
7. محمد آل فرج الطائي، **"الموسوعة الكاملة في نظم المعلومات الإدارية الحاسوبية "**، دار زهران، الأردن، 2002.
8. محمد بن أحمد بن تركي السديري، **"نظم المعلومات الإدارية"**، جامعة الملك سعود، 2012.
9. مروان العبد محمد أبو زعنونة و علاء الدين محمد الصويتي، **"مقدمة في أمن الشبكات"**، دار المعتز، الأردن، 2009.
10. هويدا علي عبدالقادر، **"نظم المعلومات الإدارية النظرية والتطبيق "**، دار الجنان للنشر والتوزيع، الخرطوم، 2011.

II. البحوث الجامعية:

أ. مذكرات ماجستير:

1. حرية شعبان الشريف، **"مخاطر نظم المعلومات المحاسبية الإلكترونية :دراسة تطبيقية على المصارف العاملة في قطاع غزة"**، مذكرة ماجستير، الجامعة الإسلامية غزة، 2006.
2. سعد بن عبد الهادي بن جليغم، **تقويم الدور الرقابي لهيئة الاتصالات وتقنية المعلومات السعودية في الحد من المخاطر الأمنية لاستخدامات مواقع التواصلالاجتماعي**، رسالة ماجستير في العلوم الإدارية غير منشورة، جامعة نايف العربية للعلوم الأمنية ، العربية السعودية، 2014.

3. علي حسين أحمد الحمادي، **"أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية"**،مذكرة ماجستير، جامعة الشرق الأوسط، الأردن 2010

4. غانم بن غزاي الروقي العتيبي، **"أمن نظم المعلومات وعلاقته بمستويات الإبداع للعاملين في شركة الاتصالات السعودية بالرياض"** ، رسالة ماجستير في العلوم الإدارية غير منشورة، جامعة نايف العربية للعلوم الأمنية، السعودية

5. فاطمة ناجي العبيدي، **"مخاطر استخدام نظم المعلومات المحاسبية المحوسبة و أثرها على فاعلية عملية التدقيق في الأردن"**، رسالة ماجستير في المحاسبة، جامعة الشرق الأوسط، الأردن، 2012.

6. لونيس نادية، **"أثر تكنولوجيا المعلومات والإتصالات في تفعيل الأعمال التجارية للمؤسسات "**، مذكرة ماجستير غير منشورة ، جامعة الجزائر3 ، 2011/2010".

ب. مذكرات ماستر:

1. آسيا قاسمي،**"أثر التقييم المالي للمشاريع الإستثمارية على إتخاذ القرار الإستثماري في المؤسسات الإقتصادية– دراسة عينة من المشاريع للفترة2003–2014"**،مذكرة ماستر غير، جامعة ورقلة، 2014–2015.

2. لمياء بوطبة، **"محاولة تدقيق نظام معلومات المؤسسة الوطنية للجيوفيزياء-ENAGEO- بحاسي مسعود ولاية ورقلة"**،مذكرة ماستر غير منشورة، جامعة ورقلة، 2015/2014.

III. أوراق بحثية :

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

IV. المحاضرات :

1. خالد رجم، ، **"محاضرات أمن نظم المعلومات"**، مقياس مراجعة نظام المعلومات، أولى ماستر، جامعة ورقلة، 2015–2016.

ثانيا : المراجع باللغة الأجنبية

I. الكتب :

1. Oihab Allal-Chérif et Olivier Dupouet, **« Optimisez votre Système d'Information « vers la PME numérique en réseau »**, Afnor ,saint-denis, France, 2014.
2. Robert Reix, Bernard Fallery, Michel Kalika et Frantz Rowe**, « Système d'information et gestion des organisations »**, 6 edition, Vuibert, paris , 2011.
3. Téphane Bourliataux, Cyril Gallitre & Yvers Roy, **« Systèmes d'information de gestion »,** Dunod, paris, 2008.

II. البحوث الجامعية

1. DOREEN MORAA NYAMONGO**, « Information systems security management a case of private chartered universities in Kenya »**, Thesisof Master of Science in Information Technology at Strathmore University, Kenya,2012.
2. Kelemie Tebkew Yirdaw**, « Information security management framework for banking industry in Ethiopia »,** Thesis of Master degree of science in information science, Ethiopia, 2013.
3. MWITA SIMION MAROA, **« Factors affecting information systems security effectiveness in university of Nairobi »,**Thesis of Master of science degree in information systems, Kenya,2015.

ثالثا : مواقع الانترنت

1. http://www.dralmarri.com/
2. https://www.algerietelecom.dz/
3. http://www.digitato.it/

الملاحق

الملحق رقم (01): الإستبيان

جامعة قاصدي مرباح ــ ورقلة ــ

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قسم علوم التسيير

تخصص : تدقيق ومراقبة التسيير

نضع بين أيديكم هذا الاستبيان، والذي يندرج في إطار تحضير مذكرة ماستر أكاديمي تخصص تدقيق ومراقبة التسيير ، الموسومة بعنوان

تقييم مدى مساهمة أمن نظم المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات
دراسة حالة مؤسسة إتصالات الجزائر- ورقلة خلال الفترة2015/2016

كما نحيطكم علماً أن استخدام هذه الإجابات سوف يكون فقط لأغراض البحث العلمي، مع ضمان السرية التامة للإجابات.

وعلى أمل تعاونكم تقبلوا منا فائق الاحترام، وشكراً مسبقاً.

يمكنكم الحصول على نسخة من ملخص نتائج البحث بالاتصال عبر البريد الإلكتروني: mastereogx@gmail.com

رقم الاستبيان: | | | |

نطلب منكم وضع علامة (X) في الخانة المناسبة

الجنس : ذكر ☐ أنثى ☐

المستوى التعليمي : ابتدائي ☐ متوسط ☐ ثانوي ☐ تقني سامي ☐ جامعي ☐

الوظيفة عامل تنفيذي ☐ عامل تحكم ☐ إطار ☐ إطار سامي ☐

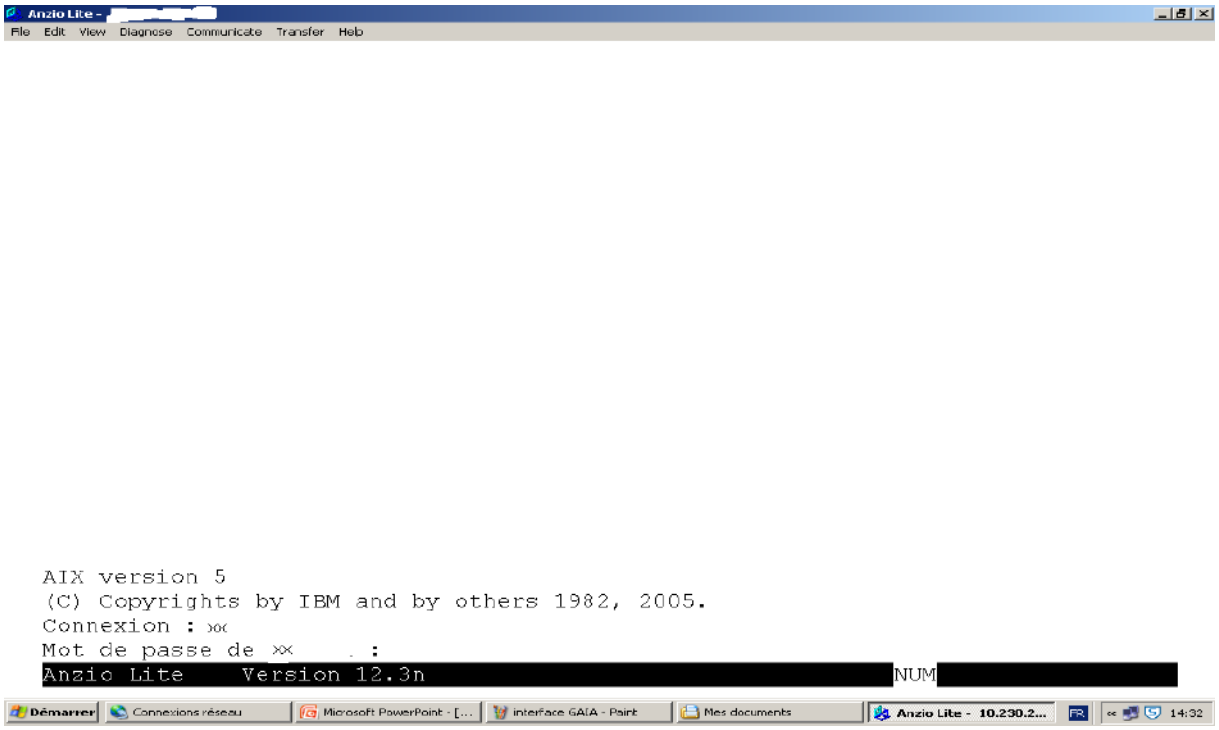
الخبرة (بالسنوات) أقل من 5 ☐ بين 5 إلى10 ☐ بين 11 إلى15 ☐ بين 16 إلى 20 ☐ أكثر من 20 ☐

نظام المعلومات في المؤسسة : يدوي لا يستخدم الكومبيوتر ☐ يعتمد على الكمبيوتر بصفة كبيرة ☐ مشترك ☐

	مخاطر تهدد نظم المعلومات	غير موافق	موافق بشكل متوسط	موافق
البعد الأول : المدخلات				
1	هناك اخطاء غير متعمدة اثناء ادخال المعلومات			
2	تعرض النظام الى ادخال بيانات خاطئة عمدا لاغراض معينة			
3	يشترك الموظفون في المصلحة بكلمة سر واحدة			
4	يستعمل الحوامل الخارجية فلاش ديسك لإدخال البيانات			
البعد الثاني : المعالجة				
5	تعرض إلى هجمات فيروسية من داخل الشبكة			
6	تعرض إلى هجمات فيروسية من خلال شبكة الانترنت			
7	توقف(تعطل) النظام بسبب خلل في الشبكة			
8	توقف(تعطل) النظام بسبب خطأ في استعمال الأجهزة			
البعد الثالث : المخرجات				
9	إنشاء مخرجات مزيفة مشابهة للأصل التي تستخرج بواسطة النظام			
10	الوصول غير المرخص للبيانات من طرف الموظفين			
11	الوصول غير مرخص للبيانات من طرف أفراد خارج المؤسسة			
12	طمس أو تدمير بنود من المخرجات			

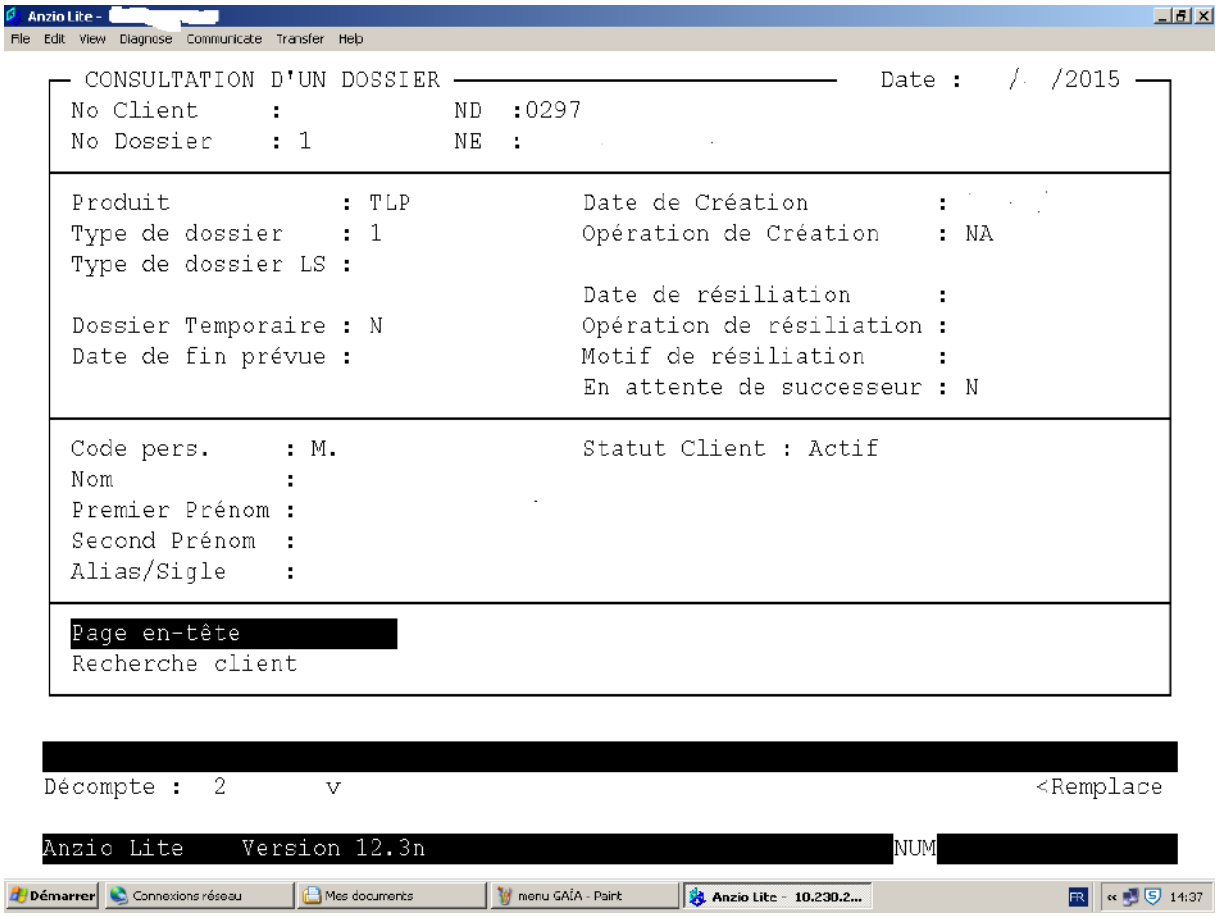
	السياسات الأمنية المتبعة	غير موافق	موافق بشكل متوسط	موافق
البعد الأول : السرية أو الموثوقية CONFIDENTIALITY				
1	يتم إدخال المعلومات بعد مصادقة المسئول المباشر			
2	يتم تحسيس الموظفين بمخاطر نظم المعلومات			
3	يتم تكوين العمال عند تحديث النظام			
4	المكان المخصص لأجهزة ربط الشبكة مؤمن ولا يسمح لغير المختصين بالوصول إليه			
البعد الثاني : التكاملية وسلامة المحتوى INTEGRITY				
5	يتم تثبيت مضادات الفيروسات والتحديثات المتعلقة بها			
6	يتم منع الدخول لمواقع انترنت محددة بطريقة مركزية			
7	تحتوي الشبكة على جدار ناري يمنع التسلل عبرها			
8	لا يسمح بتثبيت البرامج المقرصنة وغير المرخصة			
البعد الثالث : استمرارية توفر المعلومات او الخدمة AVAILABILITY				
9	يتم صيانة الشبكة دوريا			
10	يتم عمل نسخ احتياطيّ للبيانات			
11	يتدخل المختصين بكفاءة لإصلاح أي عطل			
12	يتم تغيير الأجهزة دوريا لتوافق أخر التطورات التكنولوجيات			
البعد الرابع : عدم الإنكار Non-repudiation				
13	يتم تغيير كلمة المرور دوريا			
14	يتم التصريح بعناوين الحواسيب (IP) حتى يتم الدخول للنظام			
15	تسجل أي عملية أثناء المعالجة بإسم المستخدم الذي قام بها			
16	الحواسيب محمية بكلمات مرور شخصية			

الملحق رقم (02): نافذة الدخول للبرنامج



الملحق رقم (03): قائمة البرنامج

الملحق رقم (04): نافذة من البرنامج



الملحق رقم (05): الفا كرونباخ (المخاطر)

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,742	12

الملحق رقم (06): الفا كرونباخ (الامن)

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,806	16

الملحق رقم (07): الفا كرونباخ (الكلي)

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,772	28

الملحق رقم (08): مخرجات الجنس

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	ذكر	46	51,1	51,1	51,1
	أنثى	44	48,9	48,9	100,0
	Total	90	100,0	100,0	

الملحق رقم (09): المستوى التعليمي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	متوسط	6	6,7	6,7	6,7
	ثانوي	24	26,7	26,7	33,3
	تقني سامي	22	24,4	24,4	57,8
	جامعي	38	42,2	42,2	100,0
	Total	90	100,0	100,0	

الملحق رقم (10): الوظيفة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	عامل تنفيذي	36	40,0	40,0	40,0
	عامل تحكم	12	13,3	13,3	53,3
	إطار	39	43,3	43,3	96,7
	إطارسامي	3	3,3	3,3	100,0
	Total	90	100,0	100,0	

الملحق رقم (11): الخبرة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	أقل من 5 سنوات	11	12,2	12,2	12,2
	من 5 إلى10	25	27,8	27,8	40,0
	من 11 إلى15	29	32,2	32,2	72,2
	من 16 إلى 20 سنة	13	14,4	14,4	86,7
	أكثرمن 20 سنة	12	13,3	13,3	100,0
	Total	90	100,0	100,0	

الملحق رقم (12): نظام المعلومات في المؤسسة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	يعتمد على الكمبيوتر بصفة كبيرة	87	96,7	96,7	96,7
	مشترك	3	3,3	3,3	100,0
	Total	90	100,0	100,0	

الملحق رقم (13): المتوسطات الحسابية (الامن- السرية أو الموثوقية)

Statistiques descriptives

	N	Moyenne	Ecart type
يتم إدخال المعلومات بعد مصادقة المسئول المباشر	90	2,44	,672
يتم تحسيس الموظفين بمخاطرنظم المعلومات	90	2,26	,787
يتم تكوين العمال عند تحديث النظام	90	2,64	,567
المكان المخصص لأجهزة ربط الشبكة مؤمن ولا يسمح لغيرالمختصين بالوصول إليه	90	2,42	,764
السريةأوالموثوقية	90	2,3500	,57304
N valide (liste)	90		

الملحق رقم (14): المتوسطات الحسابية (الامن- التكاملية سلامة المحتوى)

Statistiques descriptives

	N	Moyenne	Ecart type
يتم تثبيت مضادات الفيروسات والتحديثات المتعلقة بها	90	2,10	,794
يتم منع الدخول لمواقع انترنت محددة بطريقة مركزية	90	2,42	,779
تحتوي الشبكة على جدار ناري يمنع التسلل عبرها	90	2,48	,657
لا يسمح بتثبيت البرامج المقرصنة وغير المرخصة	90	2,38	,728
التكاملية وسلامة المحتوى	90	2,3444	,52142
N valide (liste)	90		

الملحق رقم (15): المتوسطات الحسابية (الامن- الاستمرارية)

Statistiques descriptives

	N	Moyenne	Ecart type
يتم صيانة الشبكة دوريا	90	2,16	,733
يتم عمل نسخ احتياطية للبيانات	90	2,50	,604
يتدخل المختصين بكفاءة لإصلاح أي عطل	90	2,39	,665
يتم تغيير الأجهزة دوريا لتوافق أخر التطورات التكنولوجيات	90	2,29	,674
الاستمرارية	90	2,3333	,47107
N valide (liste)	90		

الملحق رقم (16): المتوسطات الحسابية (الامن- عدم الانكار)

Statistiques descriptives

	N	Moyenne	Ecart type
يتم تغيير كلمة المرور دوريا	90	2,18	,696
يتم التصريح بعناوين الحواسيب (IP) حتى يتم الدخول للنظام	90	2,63	,644
تسجل أي عملية أثناء المعالجة بإسم المستخدم الذي قام بها	90	2,76	,504
الحواسيب محمية بكلمات مرور شخصية	90	2,37	,694
عدم الانكار	90	2,4833	,37626
N valide (liste)	90		

الملحق رقم (17): المتوسطات الحسابية (المخاطر-المدخلات)

Statistiques descriptives

	N	Moyenne	Ecart type
هناك اخطاء غير متعمدة اثناء ادخال المعلومات	90	2,10	,688
يتعرض النظام الى ادخال بيانات خاطئة عمدا لاغراض معينة	90	1,29	,604
يشترك الموظفون في المصلحة بكلمة سر واحدة	90	1,49	,753
يستعمل الحوامل الخارجية فلاش ديسك لإدخال البيانات	90	1,99	,828
المدخلات	90	1,7167	,43576
N valide (liste)	90		

الملحق رقم (18): المتوسطات الحسابية (المخاطر-المعالجة)

Statistiques descriptives

	N	Moyenne	Ecart type
تعرض إلى هجمات فيروسية من داخل الشبكة	90	1,93	,667
تعرض إلى هجمات فيروسية من خلال شبكة الانترنت	90	1,72	,808
توقف) تعطل (النظام بسبب خلل في الشبكة	90	2,14	,712
توقف)تعطل (النظام بسبب خطأ في استعمال الأجهزة	90	1,93	,700
المعالجة	90	1,9333	,45252
N valide (liste)	90		

الملحق رقم (19): المتوسطات الحسابية (المخاطر-المخرجات)

Statistiques descriptives

	N	Moyenne	Ecart type
إنشاء مخرجات مزيفة مشابهة للأصل التي تستخرج بواسطة النظام	90	1,44	,638
الوصول غير المرخص للبيانات من طرف الموظفين	90	1,38	,628
الوصول غير مرخص للبيانات من طرف أفراد خارج المؤسسة	90	1,30	,608
طمس أو تدمير بنود من المخرجات	90	1,39	,555
المخرجات	90	1,3778	,51282
N valide (liste)	90		

الفهرس

الفهرس