

تقييم كفاءة نظام المعلومات الإلكتروني: دراسة مقارنة بين المؤسسة الوطنية للجيوفيزياء ومؤسسة الشراكة HESS (اجنبية- سونطراك)

evaluating the efficiency of the electronic information system : a comparative study between ENAGEO and HESS

أ. ذكار محمد يزيد

جامعة غرداية – الجزائر

y.dokk2009@gmail.com

د. رجم خالد / أ.بن عمارة الطاهر

جامعة ورقلة – الجزائر

tahaer.benamara@gmail.com / Redjemkhaled@gmail.com

تاريخ النشر: 2018/12/31

تاريخ القبول: 2018/12/11

تاريخ الإرسال: 2018/09/24

الملخص:

تهدف هذه الدراسة الى تقييم كفاءة نظام المعلومات الإلكتروني في المؤسسة الوطنية للجيوفيزياء، مقارنة مع المؤسسة الاجنبية HESS (امريكية-جزائرية) ، من حيث المعايير: (موارد بشرية، مكونات مادية (Hardware)، قواعد وبرمجيات (Software)، جودة المعلومات، وأهمية تدقيق نظام المعلومات في المؤسسة)، وخلصت الدراسة الى وجود عدة نقاط ضعف في المؤسسة الوطنية للجيوفيزياء بما يتعلق بعدم الاستغلال الأمثل لموارد النظام اضافة الى غياب التطبيق الصارم للعقوبات المتعلقة بنظام المعلومات، كما وجدنا غياب تام للأخذ بعين الاعتبار التوصيات المقدمة من طرف المدقق المتعلقة بنظم المعلومات، بالمقارنة مع الشركة الاجنبية HESS فهي تتميز بمستوى عالي من حيث الاستغلال الأمثل لموارد نظام المعلومات، واهمية تقارير المدقق المتعلقة بنظم المعلومات.

- الكلمات المفتاحية : نظام المعلومات الإلكتروني، أمن نظام المعلومات، تدقيق نظام المعلومات، مخاطر نظم المعلومات.
- تصنيف JEL: M15، M42.

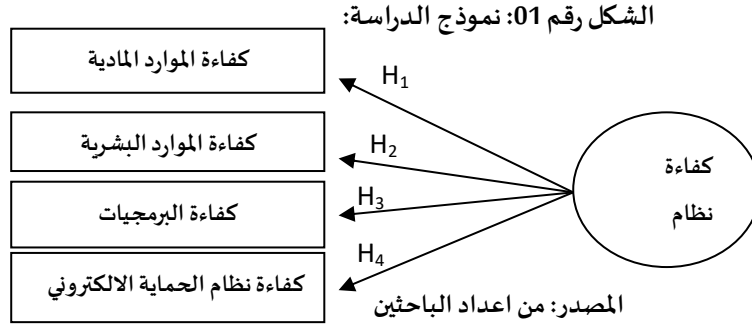
Abstract:

This study aims at evaluating the efficiency of the electronic information system at the National Corporation of Geophysics [Entreprise Nationale de Géophysique (ENAGEO)] in comparison to the Americo-Algerian corporation HESS, and it focuses on the following criteria : (human resources, hardware, software, quality of information, and the importance of information system audit in the corporation).. The findings of the current study show that the Entreprise Nationale de Géophysique has several weaknesses related to the lack of optimal use of the system's resources along with the absence of strict application of penalties. This study also finds out that there is total lack of taking the auditor's recommendations concerning the information systems into consideration. The foreign company HESS, on the other hand, is concluded to have a high level in terms of the optimisation of information system resources and the importance of auditor's.

- **Keywords :** E- Information System, IS Security, IS Audit, IS Risks.
- **(JEL) Classification :** M15: M42

تمهيد:

ان واقع التسيير في المؤسسات الوطنية يعاني بعض العجز رغم احتكاكنا بمجموعة كبيرة من المؤسسات الأجنبية في إطار الشراكة، أو عن طريق المقاولات من الباطن، ولمدة زمنية معتبرة، ولكن لم ينعكس هذا على مستوى التسيير وهذا راجع لعدة أسباب، أهمها ذهنيات الإدارة والخلفيات التاريخية وعدم الاهتمام بالجانب البشري بالقدر الكافي، وعدم إعطاء الأهمية اللازمة لنظام المعلومات، وعدم تفعيل دور التدقيق لتحقيق التكيّف والاستمرارية في ظل التغيرات المتسارعة للتقنيات والتكنولوجيات من أجل الوصول إلى تحقيق كفاءة نسبية مقبولة، وعلى ضوء ما سبق نصل إلى طرح إشكالية بحثنا: ما مدى كفاءة نظام المعلومات الالكتروني في المؤسسات محل الدراسة من حيث موارد النظام؟



فرضيات الدراسة.

الفرضية الاولى: تتوفر المؤسسات على مكونات نظام المعلومات مادية (Hardware) كافية وحديثة.
الفرضية الثانية: تتوفر المؤسسات على موارد بشرية كافية ومؤهلة لتسيير واستخدام النظام، وتستفيد دوريا من برامج تكوين وتأهيل تتلاءم ومتطلبات نظام المعلومات المستخدم.
الفرضية الثالثة: تتوفر المؤسسات على برمجيات (Software) حديثة وقابلة للتحديث تساهم في فعالية نظام المعلومات.
الفرضية الرابعة: تتوفر المؤسسات على نظام حماية الكتروني يحافظ على موارد النظام، ويضمن أمن وسرية المعلومات.
أهداف البحث:

1. توضيح مدى مساهمة كفاءة نظام المعلومات الالكتروني في تحسين المعاملات الإدارية؛
2. إظهار مشاكل ومعوقات تطبيق نظام معلومات كفو في المؤسسات الوطنية بالمقارنة مع الأجنبية؛
3. محاولة الوصول لتوصيات حول اشكاليات الاستغلال الأمثل لنظم المعلومات في المؤسسات الوطنية مقارنة بالأجنبية.

منهج الدراسة:

اعتمدنا في الجانب التطبيقي على منهج دراسة الحالة من خلال تحليل واقع نظام المعلومات المعتمد (العتاد، البرامج، الشبكات، الاجراءات، المستخدمين)، إضافة الى المقابلة مع مسيري ومستخدمي نظام المعلومات في المؤسسة لمعرفة مدى كفاءة النظام و ماهي اهم معوقات الاستغلال الأمثل للنظام.

محاور البحث:

- المحور الأول: مدخل لنظام المعلومات؛
- المحور الثاني: تدقيق نظام المعلومات ؛
- المحور الثالث: الجانب التطبيقي؛

أولاً: مدخل لنظام المعلومات

1- تعريف نظام المعلومات: يمكن تعريف نظام المعلومات تقنيا كمجموعة من المكونات المترابطة تهدف إلى تجميع ومعالجة وتخزين وتوزيع المعلومات لدعم القرار والتحكم في المؤسسة وبإضافة إلى دعم عملية صنع القرار، والرقابة والتنسيق والسيطرة، فإن نظم المعلومات تساعد أيضا الإدارة العليا على تحليل المشاكل بتوفير المعلومات المناسبة في الوقت المناسب¹.

2- أهمية نظام المعلومات في المؤسسة:

- أ- تزايد نفوذ المعرفة والمعلومات في المجتمعات الصناعية الحديثة لذلك نجد إن إنتاجية المشتغلين بالمعلومات أصبحت احد الاهتمامات الرئيسية في المجتمعات الغربية، مما أدى إلى زيادة الطلب على المعلومات.
 - ب- تنمية وتطور شبكات الاتصال والمعالجة الدقيقة، فقد أدى ظهور نظم المعلومات الإلكترونية إلى زيادة الطلب على استخدامها لدرجة يمكن تواجد منظمات تعمل بالكامل بواسطة الحاسب الآلي وشبكة معلومات واحدة.
 - ت- التغيرات التي طرأت على طلب المعلومات والأساليب الفنية اللازمة لتشغيلها إذ تعتبر موردا استراتيجيا مهما.
- 3- أمن نظام المعلومات :

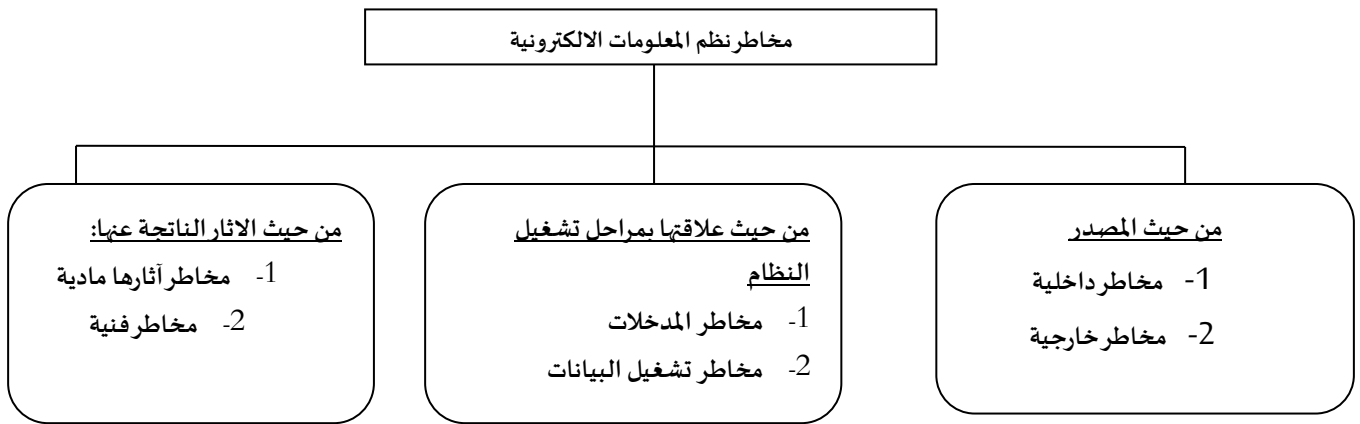
هو جميع الطرق والتقنيات ووسائل الأمن والحماية لموارد نظام المعلومات، ويمثل الهدف من أي برنامج امن يعد لنظام المعلومات حماية المنظمة وذلك بتقليل المخاطر التي تؤثر على توافر المعلومات وسريتها وسلامتها بمستوى مقبول ومحدد²، وعليه يجب على المؤسسة وضع قواعد السلامة وإتباع السياسات الأمنية وفق المعايير لضمان السير السليم للنظام³، وينبغي ان يتضمن التخطيط والرقابة الإدارية على امن النظام ما يلي⁴:

- تحديد الأهداف والتي تعتبر بمثابة معايير لتقييم امن النظام فيما بعد، وتتمثل هذه الأهداف في حماية مكونات النظام؛
- تقدير الاحتمالات والتكاليف المرتبطة بمخاطر امن تشغيل البيانات؛
- إعداد خطة تضمن مستوى مقبولا من الأمن وبتكلفة معقولة، وتصف هذه الخطة كافة الإجراءات الرقابية التي سيتم تطبيقها وأهداف هذه الإجراءات، هذا وينبغي إن يتم فحص الخطة والتصديق عليها قبل وضعها موضع التنفيذ؛
- تحديد المسؤوليات عن امن النظام؛
- اختبار إجراءات الرقابة على امن النظام، وذلك للتحقق من مدى فعاليتها في تحقيق أهدافها المرجوة.

4- مخاطر نظام المعلومات:

يمكن تلخيص اهم المخاطر المتعلقة بنظم المعلومات الالكترونية في الشكل الاتي:

الشكل رقم 02: تصنيف مخاطر نظم المعلومات الالكترونية



المصدر: اعداد الباحثين

• لضمان أمن نظام المعلومات يجب دراسة وتحليل العناصر التالية:

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 صنفت تلك العناصر إلى خمسة عناصر وهي⁵:

- ✓ التحقق من المستعمل: التأكد من هوية الشخص الذي يستخدم المعلومات، عن طريق فحص الصلاحيات الإلكترونية لكل مستخدم.
- ✓ سلامة المحتوى: أي التأكد من أن محتوى المعلومات صحيح ولم يحرف، ولتفادي ذلك يجب على المؤسسة تأمين سلامة المحتوى من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات والفيروسات.
- ✓ استمرارية توفر المعلومات أو الخدمة: سلامة وأمن التخزين والاسترجاع تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل وتقديم الخدمات لمستخدمين المرخص لهم بها، ومنع استخدامها أو الوصول إليها بطرق غير مشروعة.
- ✓ - المسؤولية: إمكانية تتبع الأثر في حالات التغيير والتحريف والحذف. ويقصد به ضمان توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص في وقت معين.
- ✓ السرية أو الموثوقية: أي التأكد من أن المعلومات لا يمكن الاطلاع عليها من قبل أشخاص غير مصرح لهم.

ثانياً: تدقيق نظام المعلومات

1- تعريف تدقيق نظام المعلومات (Audit Information system): إن تدقيق نظام المعلومات يشمل كل مراحل دورة حياة النظم انطلاقاً من عملية التخطيط إلى المتابعة للأنشطة والعمليات التحويلية والتصميمية والتطبيقية لنظام المعلومات. وعليه فإن عملية الرقابة تعمل على مراقبة ومراجعة وتصحيح الأخطاء وكشف الانحرافات بصورة مستمرة في كل المراحل بهدف تقليل المخاطر وتحسين الأداء باستمرار، بالإضافة إلى سلامة وأمن المكونات المادية للنظام وكذا البرامج وهذا كله في إطار تكاليف معقولة ومسموح بها.

إن تدقيق نظام المعلومات يمكن من التأكد من أن كل الوسائل والعمليات والأنشطة الخاصة بالنظام تسيير بالشكل الصحيح مقارنة مع المخططات والأهداف.⁶

أن تدقيق نظام المعلومات يتضمن تحديد جميع الضوابط التي تحكم نظام المعلومات وتقييم فعاليته، وللقيام بذلك، يجب على المدققين مراجعة كافة مكونات النظام، وكذلك تقييم أمن النظام وتحليل المخاطر المتعلقة به.⁷

2- أهداف تدقيق نظام المعلومات :

تأسس الأهداف العامة لمراجعة نظم المعلومات على ما يلي:⁸

- زيادة الثقة : فهي تعطي الثقة المستمرة كفاءة المعدات وطبيعة معالجة العمليات وبالتالي تكون البيانات صحيحة ودقيقة وكاملة وأمنة.

- صحة الإجراءات : بمعنى أن إجراءات المعالجة صحيحة وفعالة أثناء جميع مراحل تشغيل النظام.

- تأكيد الدقة : أي أن النظام ينتج معلومات مالية أو أي معلومات أخرى تتميز بالدقة.

- الكفاءة والفعالية: أي وجوب تقييم تكلفة الكفاءة والفعالية للنظام وإن كانت أجهزة النظام أو البرامج

تقدمان خدمة مرضية وتلبي حاجات المستفيدين.

التحقق من أن النظم الموضوعة تعمل بشكل صحيح، وأنها تحقق الغرض الذي وضعت من أجله ويمكن تناول

أهداف مراجعة نظم المعلومات الإلكترونية في النقاط التالية⁹:

- التأكد من فعالية الرقابة الداخلية للبيانات ولأجهزة وشبكات التوصيل وكفاية الحماية:

- التأكد من أن امتلاك البرامج وتطويرها يتم بترخيص؛
- التأكد من أن أي تعديل للبرنامج يتم بموجب تفويض الإدارة؛
- التأكد من أن معالجة العمليات والملفات والتقارير وأي سجلات إلكترونية أخرى تتم بدقة وبشكل كامل؛
- التأكد من أن البيانات المصدرة التي بها أخطاء يتم تمييزها ثم معالجتها طبقاً لسياسات الإدارة؛
- التأكد من أن ملفات نظام المعلومات الإلكتروني تتميز بالدقة والاكتمال والسرية.

3- ما يجب تدقيقه وتقييمه في نظام المعلومات (مكونات نظام المعلومات):

سنلخص ما يجب تدقيقه وتقييمه من جانب مكونات نظام المعلومات في الشكل الموالي:

الشكل رقم (3): عناصر تدقيق وتقييم مكونات نظام المعلومات.



المصدر: من اعداد الباحثين بناء على¹⁰ ،¹¹

4- أساليب الرقابة على نظام المعلومات المحوسب:

تعد أساليب الرقابة أكثر أهمية في نظم المعلومات الإلكترونية عن تلك المتبعة في النظم اليدوية لعدة أسباب أهمها:¹²

1. يتم معالجة قدر كبير من البيانات بواسطة الكمبيوتر يفوق تلك التي تعالج يدوياً مما ينتج عنه زيادة احتمال ارتكاب أخطاء؛
2. يتم جمع ومعالجة وتخزين بيانات العمليات في صورة غير قابلة للقراءة لا يمكن للإنسان مراقبة هذه البيانات والتحقق من دقتها وموضوعيتها والتي كان يسهل إجرائها تحت النظام اليدوي للمعلومات؛
3. يصعب تتبع مسار التدقيق مما قد يترتب عليه احتمال قيام الموظفين غير الأمناء باختلاس مبالغ طائلة من الوحدات الاقتصادية التي يعملون بها.

وتقسم غالباً أساليب الرقابة على التطبيقات إلى ثلاثة مجموعات وهي: أساليب الرقابة على المدخلات وأساليب الرقابة على معالجة البيانات وأساليب الرقابة على المخرجات:

1. أساليب الرقابة على المدخلات Input Control :

تهدف إلى توفير درجة تأكد معقولة من صحة اعتماد البيانات التي يتسلمها قسم معالجة البيانات EDP بواسطة موظف مختص ومن سلامة تحويلها بصورة تمكن الكمبيوتر من التعرف عليها. ومن عدم فقدانها أو الإضافة إليها أو حذف جزء منها أو

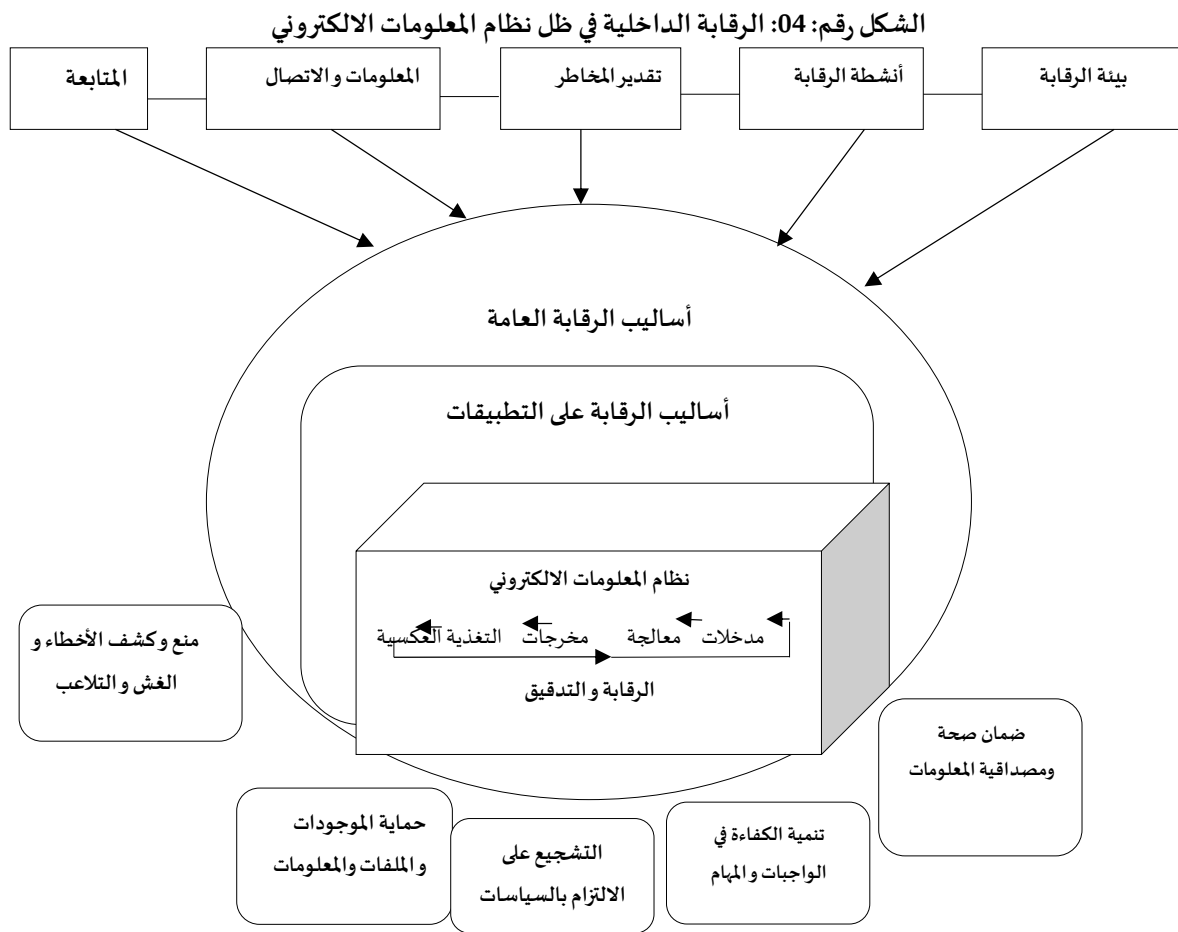
طبع صورة منها أو عمل أي تعديلات غير مشروعة في البيانات المرسله حتى وان كان ذلك من خلال خطوط الاتصال المباشرة. وتشمل أساليب الرقابة على المدخلات على تلك الأساليب التي تتعلق برفض وتصحيح وإعادة إدخال البيانات السابقة.

2. أساليب الرقابة على معالجة البيانات Processing Control :

وتهدف إلى توفير درجة تأكد معقولة من تنفيذ عمليات معالجة البيانات إلكترونياً طبقاً للتطبيقات المحددة، بمعنى معالجة كافة العمليات كما صرح بها وعدم إغفال معالجة عمليات صرح بها وعدم معالجة أي عمليات لم يصرح بها.

3. أساليب الرقابة على المخرجات Out Put Control :

وتهدف إلى تأكيد دقة مخرجات عمليات معالجة البيانات (مثل قوائم الحسابات أو التقارير أو أشرطة الملفات الممغنطة أو الشبكات المصدرة) وتداول هذه المخرجات بواسطة الأشخاص المصرح لهم فقط بذلك.



المصدر: ألان عجيب، نادر صبري، دور الرقابة الداخلية في ظل نظام المعلومات المحاسبي الالكتروني دراسة تطبيقية على المصارف في إقليم كردستان، مجلة علوم إنسانية، العدد 45، العراق، 2010، ص5

الجدول رقم (1) : مقومات نجاح واسباب فشل نظام المعلومات الادارية من وجهة نظر الباحثين.

الباحث	مقومات نجاح نظام المعلومات	أسباب فشل نظام المعلومات
Bruwer 1984	مشاركة المستفيد، مساندة الإدارة العليا، لعناصر الشخصية، اتجاه المديرين نحو النظم الآلية.	يعتبر فشل لنظام المعلومات عند عجز النظام عن الأداء بالصورة المتوقعة، أو عدم قدرته على تنفيذ عملياته في التوقيتات المحددة، أو عدم إمكانية استخدامه على النحو الذي احضر او صمم من أجله
Gerhard19 88	إسهام المستفيدين من تصميم النظام، تحديد البرمجيات ومعرفة خصائصها قبل تحديد نوع النظم، ينبغي البدء بتحليل المخرجات المعلوماتية وتحديد نوع المستفيد لمعرفة المدخلات ثم تحصيل مصادر الحصول على البيانات وأخيراً تحديد طريقة المعالجة.	- عدم دعم الإدارة العليا او الإدارة التنفيذية - عدم اشراك المستفيدين وتحديد نوع احتياجاتهم - الاهتمام بالأجهزة وليس بالأهداف
باغي 1988	الفهم السليم لطبيعة النظام ورسالته، تحديد نوعية الاحتياجات من المعلومات وكميتها، وجود مقياس لمدى قدرة المدير على توظيف، تفهم المدير لعمل نظام المعلومات الإدارية المعلومات.	- سوء تحديد الاحتياجات من المعلومات - عدم الدقة بطلب موارد المعلومات بنفس درجة الحرص التي تطلب بها الموارد الأخرى
خشبة 1995	خصائص متخذ القرار، خصائص نظام المعلومات، خصائص بيئة القرار، خصائص عملية التنفيذ.	- عدم توافر القدرات البشرية الملائمة من مستخدمين ومتخصصين
السالي 1999	محلل النظام والذي يعد حافزاً للتغيير وضمان نجاح النظام، تفاعل المستخدم، قوة الاتصال بين المستخدم والمصمم، دعم الإدارة .	- صعوبة الاتصال والتفاعل بسبب تباين الخلفية التعليمية والثقافية بين أخصائي نظم المعلومات ومستخدميه -كبر نسبة المخاطرة والتعقيد وتكلفة النظام
سلطان 2000	اشتراك المستخدم النهائي، دعم الإدارة، مستوى التعقيد والمخاطرة، إدارة عملية التنفيذ .	- افتقار الصيانة الملائمة حسب المورد.
Aman jindal 2003	ارتباط المستخدم، دعم الإدارة التنفيذية، توقعات واقعية، تخطيط ملائم، متطلبات واضحة .	

المصدر: احمد مؤيد عطية الحيايى د. نجله يونس محمد ال مراد " مؤشرات نجاح نظام المعلومات الإدارية ودورها في الإبداع والتميز" المؤتمر العلمي الثالث لكلية الاقتصاد والعلوم الادارية جامعة العلوم التطبيقية الخاصة "إدارة منظمات الأعمال: التحديات العالمية المعاصرة" 2009 م الاردن، ص 9.

المحور الثالث: الجانب التطبيقي

1- عينة الدراسة: تتمثل عينة الدراسة في المؤسستين ENAGEO و HESS.

جدول رقم (2): عينة الدراسة

اسم المؤسسة	نوع النشاط	نوع المؤسسة	تاريخ التأسيس	عدد العمال
المؤسسة الوطنية للجيوفيزياء ENAGEO	انجاز الدراسات الجيوفيزيائية لطبقات الأرض ذات البعدين، والطبقات الأرضية ذات الثلاثة أبعاد.	اقتصادية ذات طابع عمومي تابعة لمجمع سونطراك.	1966	6 307 عامل
مؤسسة HESS	هي شركة التوصية بالأسهم أمريكية متعددة الجنسيات لها عدة مجالات نشاطات عبر العالم، ولقد تم إنشاء الشراكة بين شركة HESS وشركة سونطراك سنة 2000. من نشاطاتها: - حفر الابار والإنشاء محطة تصفية الزيوت وقاعدة حياة؛ - الإستغلال: مقسم الى نسبة 51% سونطراك مقابل 49 % لشركة HESS، المدة المحددة للمشروع الى غاية 2028.	مؤسسة ناتجة عن شراكة بين سونطراك و المؤسسة الأمريكية HESS.	2012	2314 عامل

المصدر: اعداد الباحثين اعتمادا على معلومات من المؤسسات محل الدراسة

2- أدوات الدراسة:

المقابلة: تعتبر المقابلة الأداة الرئيسية التي ارتكزت عليها دراستنا في جمع المعلومات حيث اننا وضعنا برنامج لإجراء المقابلات حتى نتمكن من جمع المعلومات والمعطيات التي تساعدنا في إتمام الدراسة، و اذ قمنا باجراء مقابلة مع رؤساء المصالح المعنية (مسيري نظام المعلومات) بالاضافة الى مستخدمى النظام، حيث تضمنت كل مقابلة على مجموعة من الاسئلة حول:

1. أهمية نظام المعلومات في المؤسسة، وأهمية تطويره، وأهمية المحافظة عليه؛
 2. مكونات نظام المعلومات الالكتروني (البرامج، الموارد المادية، والكفاءات البشرية، الشبكات، قاعدة البيانات)؛
 3. المخاطر التي تهدد نظام المعلومات الالكتروني بالمؤسسة؛
 4. السياسات الأمنية المتبعة من اجل حماية امن نظام المعلومات الالكتروني بالمؤسسة؛ ودرجة الالتزام بها؛
 5. أهم المشاكل المسجلة، ودرجة خطورتها.
 6. عملية تدقيق نظام المعلومات الالكتروني في المؤسسة؛ درجة أهميتها؛
 7. الخطوات والأساليب المتبعة في عملية تدقيق نظام المعلومات الالكتروني، واهم تقاريرها ومسارها ودرجة الاهتمام بها ومراعاته؛
- تحليل واقع نظام المعلومات في المؤسستين محل الدراسة: حاولنا القيام بدراسة تحليلية شاملة لواقع نظام المعلومات الالكتروني بالمؤسستين ملخصة في الجدول التالي:

الجدول رقم (3): مقارنة واقع نظام المعلومات الإلكتروني للمؤسستين

التعيين	شركة HESS	مؤسسة ENAGEO
الكفاءات (مستعمل، ومتخصص)	جزائرية واجنبية بشهادات جامعية وخبرة حسب المنصب والمهام المسندة اليه والمسؤوليات، يتم التعيين عن طريق التحويل، او خارجي وفق شروط ومرحلة تجريب بوثيقة تقييم ممضية من عدة اطراف.	جزائرية منها ذوي شهادات جامعية، تقنيين من مراكز التكوين ومنها ذوي خبرة ومهارات مكتسبة حسب المهام المسندة.
التكوينات والتدريب	استخدام تقنية التدريب في مكان العمل وانظمة المحاكات، وجود قاعة دائمة للتكوينات (لغة، برامج، امن صناعي...) الاستاذ جزائري او اجني حسب نوع التكوين.	التدريب الاولي عند استلام المنصب، وجود قاعة دائمة للتكوينات، وجود تكوينات في قطاع اختصاص المؤسسة.
التوظيف والانتقاء	تعتمد على الخبرة بالدرجة الاولى والشهادات الجامعية	تعتمد على الشهادة وعوامل اخرى
الاستجابة وقابلية التغيير	سرعة الاستجابة لكل المستجدات، مرونة كبيرة في التغيير لان المنصب والمهام ليست مرتبطة بالجهاز وجميع الوثائق الكترونية تقريبا.	صعوبة الاستجابة ورفض التغيير، ارسيف كبير في كل مكتب وبتنظيم فردي.
الحماية	كلمة مرور لكل منصب (نظام العمل 4/4) مع اجبارية التغير كل 30 يوم، تدرج كلمة المرور ضمن تسليم المهام، قوانين صارمة تظمن الحفاض على النظام.	كلمة مرور لكل شخص، وتقوم الادارة بتغييرها بانتظام
العقوبات والمحفظات	طرد 3 مواضفين بسبب عدم مراعات شروط السلامة وثبوت التخريب، تتم بعض التقييمات مباشرة من النظام (وقت بداية العمل وقت الخروج سرعة الاجابة على الرسائل...)،	موجود وغير مطبق وغير صارم
المعدات والتجهيزات	ثلاثة خوادم متطورة اثنين منها في حالة عمل بتناوب والآخر لضمان التخزين الجيد داخل وخارج الجزائر، ثلاث طابعات مركزية ملونة حجم كبير و32 طابعة مكتبية من نفس النوع لتقليل تكاليف تخزين المستهلكات، اجهزة الكمبيوتر مكتبية لكل منصب (HP 8000, HP 8300)، 12 جهاز كمبيوتر محمول (HP Pavilion dv6 i7)، اجهزة حماية فيزيائية ضد القرصنة والفيروسات CISCO، (الجدار الناري firewall)، مولد كهرباء، وأجهزة تخزين الكهرباء Onduleurs.	عدد كافي من الخوادم كل حسب وظيفته، حواسيب شخصية من نوع (HP, Dell, Condor, Fujitsu)، طابعات مرتبطة بالشبكة من نوع HP، 134 جهاز كمبيوتر محمول، 86 ماسح ضوئي، 106 طابعة مكتبية، وأجهزة تخزين الكهرباء Onduleurs، اجهزة حماية فيزيائية ضد القرصنة والفيروسات، Firewall UTM، Modèle 1.
الشبكات الموصولة بالخادم	شبكات الداخلية LAN، شبكة كمرات المراقبة، شبكة الهاتف IPBX، شبكة الاقفال الالكترونية، و VSAT،	شبكات الداخلية LAN، و VSAT.
الحماية	CISCO، وانظمة الحماية ضد الحرائق والاندثار المبكر، وحدة تخزين كهرباء لكل جهاز كمبيوتر، بطاقة هوية الكترونية تخول لحاملها التنقل في لاماكن والاوقات المسموح له بها، مولد كهرباء.	انظمة الحماية ضد الحرائق، وحدة تخزين كهرباء لكل خادم
الصيانة ومراقبة	صيانة الشبكات اضافة وتقليص وتغيير، وبعض اعمال الصيانة البسيطة لاجهزة الكمبيوتر والطابعات، والصيانة عن بعد، ومراقبة الاستغلال، اغلب الصيانة خارج المؤسسة.	وجود دائرة صيانة بها (Helpdesk Group، Hard Maintenance Service).
البرامج	نظام التشغيل Windows 7 مرخص لكل حاسوب مكتبي. - نظام التشغيل Windows 2008-2012 Server مرخص	ويندوز Windows (XP-07) حسب معرفة مستخدم الجهاز.

الموارد البشرية
People Resources

الجانب المادي
Hardware Networks

عد والقوا

	للخوادم. - نظام ERP MAXIMO 7.0 من صنع IBM - برنامج تسيير البريد الإلكتروني Exchange - الجدار الناري: Firewal Cisco ASA	برامج مكتبية، وبرامج وظيفية منفصلة منجزة محليا، اغلب مخرجاتها ورقية، برامج مكافحة البريد المزعج ANTI-Spam، الجدار الناري: 2 و Firewal UTM Modele 1، وكذلك استخدام برنامج التشفير Cryptge، للحماية من الاختراقات، والبريد المحلي للمؤسسة (Messagerie).
	برامج حديثة ويتم تحديثها، والبعض يتم عن طريق الشركة الام كلما استدعت الحاجة لذلك، مثل ERP نسخة 2014،	برامج مكتبية منفصلة منجزة من قبل مديرية تكنولوجيا المعلومات و الاتصال يبدأ العمل بها منذ تاريخ برمجتها ويجري تحديثها كلما استدعت الضرورة لذلك.
	مضادات للفيروسات شبكية حديثة، مع قوانين تمنع نسخ وادخال معلومات من خارج الشبكة، وجود فصل واضح بين Administrator User، لا يمكن لاي User التغيير في اعدادات الجهاز .	مضادات فيروسات مكتبية مختلفة، مع ترك امكانية التوقيف للمستعمل. مضاد الفيروسات Norton / Kaspersky، برامج مضادة للقرصنة ANTI-SPYWARE
	لا تعتبر معلومة ولا تعتمد إلا اذا ارسلت بالبريد الالكتروني مثل تكليف بالانابة، طلب حجز او تغيب حجز، اعلان اجتماع غير مبرمج ...، يتم ادخالها في النظام مرة واحدة مهما كان شكلها.	عتمد على المعلومات الالكترونية مع وجود عدد كبير من المعلومات الورقية وبعض المعلومات الشفوية
المصدر:	عقود صيانة خارجية حسب الجهاز (كمبيوتر، كمرا، الة نسخ (...)	توفر الجانب الشرعي المتخصص في الصيانة
	وقائية دورية مع التحسنات عند الطلب من المستعمل، وقائية في حالة التوقف	فجائية عند التوقف
	جميع المعدات ملك للشركة بوثائق والبرامج أصلية مع المفتاح	اغلب البرامج منجزة بالمؤسسة، بعض البرامج مقتناة عن طرق النسخ
	لا يتم غلق اي اجراء مهما كان بدون الارشفة الالكترونية وجود مصلحة مختصة Doc Control،	تحفض المعلومات على مستوى المديرات كل شهر. نسخ لجميع مخرجات الوثائق على حوامل ورقية، تخزن في مقر الارشيف المكون من 6 غرف و16 مكتب وخزائن حجم كبير.
	يمنع الطباعة الا اذا استدعت الحاجة لذلك للمحافظة على البيئة، وتقليل تكاليف الطباعة	كل عملية تطبع من اجل المصادقة عليها والارشفة.

المصدر: من إعداد الباحثين بناء على المقابلات والملاحظات ومعطيات مقدمة من طرف مسؤولي نظم المعلومات في المؤسساتين

من خلال جدول و اقع نظام المعلومات في المؤسساتين تبيين النقاط التالية:

1- المورد البشري: يعتبر العمود الفقري فهو من أهم الموارد الواجب توفرها لتشغيل النظام، وعليه فان مديرية تكنولوجيا المعلومات والاتصال، توفر على أفراد ذو الخبرة والكفاءة العالية لتشغيل النظام وضمان إنجاحه موزعين على أقسامها بالمديرية الملحق رقم (3): قسم مطوري البرمجة، قسم الشبكة، قسم صيانة الأجهزة، وتقوم المؤسسة بتدريب العمال في مختلف الاختصاصات: لتدعيم الجانب البشري بالمديرية، قامت المؤسسة في جانفي 2016 بتوظيف 5 مهندسين في البرجة.

كما تظم دائرة المعلوماتية IT بمؤسسة Hess، كفاءات متميزة جزائرية وأجنبية تسهر على الرقي بمهارات المورد البشري في المؤسسة الى الدرجات التي تمكنهم من الاستخدام الجيد لنظام ERP- MAXIMO (من صنع شركة IBM)، واستعمال جميع المعدات، كما يستفيد كل افراد دائرة المعلوماتية IT من تكوينات داخل او خارج الوطن حسب الضرورة كل ستة اشهر، كل المستخدمين بدرجة الليسانس أكاديمي فما فوق، في المناصب الادارية ومهندس فمافوق في التقنية.

2-الموارد المادية (Hardware): بما ان الموارد المادية تعتبر من اهم مكونات نظام المعلومات الإلكتروني، ومن خلال الملاحظة والوثائق المقدمة فان المؤسسة تحتوي المؤسسة Enageo على اجهزة إعلام آلي متطورة تتماشى مع البرنامج المستعمل Oracle، حيث تم اقتناءها من نفس المؤسسة التي تم اقتناء منها برنامج Oracle مع ضمان معقول، وتوفر المؤسسة لكل مستعمل جهاز على مستوى كل المكاتب (Hp, Dell, Condor, Fujitsu)، طابعات رقمية متصلة بالشبكة نوع (Hp)، والات نسخ، والات طبع لكشوف الاجور، أجهزة تامين الكهرباء (Onduleur).

كما قامت المؤسسة بمنح اجهزة الحاسب محمولة لكل المسؤولين، وايضا المهندسين في مديرية (DINTIC)، بوصل استلام وتعهد بتحمل المسؤولية التامة لحماية الجهاز ومحتواه، ويسمح لهم باخراجه من المؤسسة حتى في اوقات العطل، وذلك للتواصل مع باقي العمال في حال حدوث اي مشاكل اثناء العمل والتي تتعلق بالبرنامج، فيمكن ذلك المسؤولين بتوجيه العمال عن كيفية تصليح المشكل، وهذا من اجل ضمان السير السليم للعمل.

كما يوجد على مستوى المديرية قسم صيانة الاجهزة (Département Maintenance)، وهو خاص بصيانة الاجهزة والمعدات والشبكات، واي عطل مادي او فيزيائي (Hard, Soft) في الجهاز من ناحية التشغيل يقوم القسم بالاهتمام به وتصليحه وصيانتة وكذلك حمايته من الفيروسات بتثبيت برامج مضادات الفيروسات.

اما المؤسسة الاجنبية Hess : غرفة الخوادم Serveurs محمية بقفل إلكتروني خاص يقوم بتسجيل مدة البقاء داخل الغرفة ولا يفتح إلا للأشخاص المرخص لهم أثناء أوقات العمل فقط، ومجهزة بمكيفين لضمان درجة الحرارة المناسبة داخل الغرفة، وأجهزة إنذار ضد الحرائق وأرتفاع درجة حرارة التوصيلات الكهربائية، تحتوي على خادمين يعملان بالتوازي وفي حالة حدوث عطل في أي منهما لا يشعر المستخدمين بذلك، وتوجه رسالة من الخادم قيد التشغيل إلى رئيس قسم الإعلام الآلي للتدخل، وجود خادم ثالث يقوم بمهمة التخزين الآلي للبيانات B de Stockage وذلك بالتوازي مع وحدة تخزين خارج الجزائر بمقر الشركة الأم. ومؤخرا B de Stockage جديد احتياطي (لم يركب بعد)، وجود جدار ناري عبارة عن جهاز Cisco يتم تسييره عن بعد من طرف شركة Cisco في فرنسا، وجود أجهزة تخزين الكهرباء Onduleurs من الحجم الكبير خاصة بالخوادم

3- الشبكة المعلوماتية : تسعى مديرية تكنولوجيا المعلومات و الاتصال مؤسسة Enageo، لرفع مستوى البنية التحتية لنظام المعلومات العام بهدف تلبية المتطلبات الجديدة لانجاز الانشطة والأعمال التي تتغير باستمرار. وعليه فان المؤسسة تحتوي على شبكات معلوماتية مختلفة وذلك من اجل ضمان وصول وتوفر البيانات والمعلومات المتعلقة بمختلف أنشطة المؤسسة لجميع مستخدمي البرامج والتطبيقات وهي:

- الشبكة الداخلية (Intranet): وهي متاحة لجميع الموظفين للاطلاع على القواعد والقوانين المتعلقة بالسير الحسن لمختلف الأنشطة والوظائف بالمؤسسة،

- الشبكة العالمية (Internet): وذلك قصد استفادة العمال منها، مع حجب المواقع الغير مسموح بها.

- والبريد المحلي (Messagerie): وذلك لضمان التواصل المستمر بين الموظفين ومستخدمي النظام، خاصتا بعد اعتماد البريد الإلكتروني كدليل اثبات حتى في النزاعات.

- شبكة الاتصال المحلية (Local Area Network (LAN): وهي شبكة حاسوبية محلية، تربط اجهزة الحاسوب الخاصة بالمؤسسة مع بعضها البعض ومع موزع قاعدة البيانات، لتوفير البيانات والمعلومات للمستخدمين من اجل انجاز الوظائف المختلفة.

- الشبكة الواسعة (Wan): تستخدمها كلى المؤسسات للتواصل مع جميع فروعها ومختلف الموردين والعملاء حيث قامت مؤخرا مؤسسة Enageo باستبدال الأجهزة المتعلقة بها لقدمها، وعجزها عن تلبية المتطلبات والأمن. وتم استبدالها بموجهات وجدران نارية تسمح بالدخول لمواقع مختلفة للتواصل مع مختلف المستخدمين ومواقع الانترنت بامان وموثوقية، حيث قامت المؤسسة بتدريب الموظفين بقسم الشبكة للاستخدام الجيد لهذه الأجهزة. والجدول الموالي يمثل الأجهزة التي تم استبدالها.

- بالإضافة إلى هذا تمتلك مؤسسة Hess، شبكة الاتصالات بتقنية IPBX: وهي عبارة عن محول وموزع رقمي هاتف بتقنية العنوان الالكتروني IP، يسمح بتخفيض تكاليف الاتصالات، ومراقبة الهاتف عن طريق شبكة LAN، بتقنية عالية لنقاء الصوت، ويمنع الاختراق والتجسس على المكالمات الهاتفية.

- شبكة خاصة بالأقفاال الالكترونية تعمل عم طريق البطاقات المهنية، تمكن من متابعة دخول المستخدمين إلى المؤسسة وإلى المكاتب كل حسب الصلاحيات المخصصة له، مثلا لا يمكن لأي فرد دخول غرفة الخادم إلا للمهندسي الإعلام الآلي IT، وأيضا تمكن هذه البطاقات من مراقبة قيادة السيارات التابعة للمؤسسة، واكتشاف المسؤول عن الأخطاء وتجاوزات السرعة المحددة المرتكبة والمخزنة في ذاكرة السيارة، وايضا نفسها تستعمل في الغرف - مكان إقامة المستخدمين.

- وجود شبكتي واي في Wifi ثانوية منفصلة خاصة بالاستعمال الشخصي للانترنت محمية بكلمة مرور.

3- البرنامج المستعمل:

اشترت المؤسسة Enageo سنة 2006 برنامج SGBD (Oracle) "نظام تسيير قاعدة البيانات" من المؤسسة الجزائرية ORSIMA بمبلغ 3.342.440,00 دج، ويقوم فرع نظام المعلومات بالمؤسسة بعمليات تطوير البرامج المستعملة للنظام (Oracle) على مستوى المؤسسة، أي برمجة عدة تطبيقات مختلفة⁽⁹⁾ الملحق رقم (9) وذلك بما يتناسب واحتياجات كل فرع، وكذلك القيام بمعالجة مختلف المشاكل والصعوبات التي تواجه العمال في تطبيق واستعمال البرنامج (عمليات المعالجة). والجدول الموالي يتضمن هذه التطبيقات و اهم اعمالها و تاريخ بداية تشغيلها:

الجدول رقم (4): التطبيقات المنجزة بالمؤسسة الوطنية Enageo

إسم التطبيق وتاريخه	الانجازات المحققة
Gestion des Payes 2010	حساب أجور العمال، السماح بتحويل عمليات الاجور، متابعة حالات العمال.
Gestion de la Facturation 01/01/2014	متابعة أوامر الفواتير، تتبع الفواتير، مراقبة العقود، رصد العملاء. متابعة التحويلات، متابعة شهادات الضمان، متابعة مبيعات الشركة. رصد المشاريع، الفوترة و المحاسبة.
GDPS : Gestion De Production Sismique 01/02/2014	إدارة مهام إنتاج، توحيد التقارير.
gStock 01/07/2014	متابعة طلبات الشراء، متابعة العقود مع الموردين، متابعة أوامر الشراء، متابعة اجراءات التسليم، ارجاع الطلبات للموردين، متابعة طلبات العملاء، متابعة المخرجات والتحويلات المالية، عمليات التجديد، عمليات الجرد.
Gestion des Prestataires 01/08/2014	متابعة مقدمي الخدمات، مراقبة العقود، متابعة القوانين والاجراءات، مراقبة الأجهزة، أوامر الدفع، متابعة التحويلات، متابعة بطاقات الدفع.
Gestion des Achats 01/01/2015	السماح للهيكل بمتابعة طلبات الشراء، السماح للأشخاص التابعين لإدارة تسيير المشتريات ادارة وتسيير المشتريات بشكل افضل، استخراج تقارير مباشرة من التطبيق.

المصدر: من إعداد الباحثين استنادا على معلومات مقدمة من قسم نظام المعلومات.

اما المؤسسة الاجنبية Hess فتستخدم نظام تخطيط موارد المؤسسات ERP MAXIMO 7.0 من صنع IBM:

استعملت المؤسسة نظام MAXIMO المصنع من قبل شركة المعلوماتية المتخصصة IBM⁽¹⁰⁾ الملحق رقم (10) منذ قدومها إلى

الجزائر، وهذا لما يتوفر عليه من ميزات فهو برنامج متكامل⁽¹¹⁾ الملحق رقم (11) يعمل وفق نماذج فهو نظام تقني صمم لتنسيق جميع

الموارد والمعلومات والأنشطة اللازمة لإتمام الإجراءات العملية مثل المحاسبة والموارد البشرية، وإدارة المشتريات والتخزين، كما يمكنه تبادل البيانات بين أجزائه المختلفة، وحملت المؤسسة Hess على عاتقها تكوين العمال الجزائريين الجدد على استعماله وعلى أي تحديث في البرنامج كل حسب مستلزمات وظيفته، من خلال إدراج بند التكوينات في عقد الشراكة، آخر التدريبات كانت سنة 2015 للنسخة الجديدة للنظام ERP MAXIMO 7.0، تؤخذ بعين الاعتبار في فترة التطبيق كل المشاكل واقتراحات التعديلات بعد الدراسة ترسل الى الشركة المصنعة للتعديل، كما يتمتع بخصائص أهمها: .

✓ يمكن تصميمه على حسب الطلب: فيمكنك اختيار الأجزاء التي تحتاجها فقط لإدارة شركتك دون أن تنفق أموالاً طائلة بلا جدوى، كما يمكنك تحديد صلاحيات كل مستخدم للنظام وبذلك يوفر لك مستوى جديد من الأمان لشركتك.

✓ يعد جيلاً جديداً من نظام تخطيط موارد التصنيع: حيث يعتبر نظام تخطيط موارد المؤسسات نظام متطور من نظام تخطيط موارد التصنيع (MRP) فنظام ERP يربط بين الإدارة المالية والموارد والتصنيع وخدمة العملاء وإدارتي التسويق والمبيعات.

✓ يمكن الاعتماد عليه لحل مشاكل المؤسسات: لأنه لم يصمم لتنظيم كل أقسام المؤسسة بفاعلية وكفاءة فقط بل للمساعدة أيضاً في إيجاد الحلول المناسبة لمشاكل، وذلك لضمان سلاسة عملية الإنتاج.

✓ يستخدم قاعدة بيانات موحدة: إن هذه التقنية تمكن من الربح الجيد للوقت والجهد بحيث ان المعلومة تسجل مرة واحدة، ثم تتم الاستفادة منها كل حسب ما هو مخول له من حق اطلاق أو تغيير جزئي أو كلي.

5- قاعدة البيانات: تتمثل في كل البيانات والمعلومات التي تتعلق بالنشاط سواء كان مصدرها من داخل المؤسسة او خارجها، من خلال النظام SGBD (نظام تسيير قواعد البيانات)، حيث تخزن فيه البيانات والمعلومات في شكل ملفات ومعلومات بطريقة منهجية ونظامية من عدة مصادر مختلفة يقوم بدمجها وضبطها لتسريع الاستغلال (ازالة التكرار، تحقيق استقلاليتها، سرعة الاسترداد...)، ذلك لضمان قوة وموثوقية امن المعلومات.

يتيح وجود برمجيات نظام تسيير قواعد البيانات للمستخدم امكانية التسيير السهل للبيانات والمعلومات من ناحية الانشاء، المعالجة، التخزين، وغيرها من عمليات، ويتم الدخول بصفة عامة لهذا النظام عن طريق استخدام كلمة السر.

كما تحتوي المؤسسة على مقر خاص بالارشيف، تخزن فيه كل الملفات المهمة والخاصة بالمؤسسة ويتكون من 6 غرف و16 مكتب وخزائن كبيرة الحجم. يقوم العمال في هذا القسم بمختلف عمليات التخزين للبيانات والمعلومات، سواء حوامل التخزين الالكترونية او نسخ على الاوراق، يتمتع بحماية كبيرة وممنوع الدخول اليه الا للمخولين لهم فقط، وكذلك مزود باجهزة الانذار الحريق (من خلال تصريحات المسؤولين لم تسجل اي حالة انذار حريق).

6- السياسات الامنية لحماية النظام:

- تتبع المؤسسات سياسات امنية لحماية نظام معلوماتها الالكتروني، وتتمثل في:
- كل موظف لديه كلمة سر خاصة به، وتقوم الادارة بتغييرها بانتظام.
 - غرفة الاجهزة الالكترونية (مكان تواجد الخوادم)، تحتوي على اجهزة التبريد، وكذلك اجهزة الانذار ضد الحرائق، وغير مسموح الدخول اليها الا للمخولين فقط.
 - تملك المؤسسة اجهزة تامين الكهرباء، وانذارات الحرائق، اجهزة الكترونية لاتلاف الاوراق السرية على مستوى المكاتب.
 - تنظم المؤسسة دورات تدريبية لكل مستخدم، وذلك لتطبيق قواعد ومتطلبات الامن المنصوص عليها في المؤسسة.
 - الجدران النارية: Firewall UTM Modèle 1 و Firewall UTM Modèle 2.
- وكذلك استخدام برنامج التشفير Cryptage، للحماية من هذه الاختراقات. Serveurs Proxy MS ISA 2006: حيث يقوم بالتغيير الأتوماتيكي للعناوين IP (بروتوكول الإنترنت) لتفادي دخول أشخاص الغير مصرح لهم.

- كما تستخدم المؤسسة البرامج التالية: مضادات الفيروسات Norton / Kaspersky ، برامج مضادة للقرصنة والتجسس Anti-Spyware، برامج مكافحة البريد المزعج Anti-Spam، وغيرها من برامج للحماية.
 - بالإضافة الى اجراءات الامن المتحصل عليها في اطار التعاقد مع مؤسسة ORSIMA عن طريق شراء نظم قواعد تسيير البيانات ORACLE.
 - اما بالنسبة للمؤسسة Hess :
 - لا يمكن لأي مستخدم الاستفادة من خدمة USB أو DVD إلا بترخيص من IT؛
 - كل جهاز كمبيوتر محمي من الصدمات الكهربائية عن طريق جهاز تخزين الكهرباء Onduleur؛
 - استخدام نظام متكامل للحماية والرقابة باستخدام كاميرات المراقبة والأقفال الإلكترونية للإدارة والمكاتب ، والغرف لكل مستعمل بطاقة مهنية الكترونية شخصية خاصة به؛
 - الاعتماد الكلي في الرسائل على MS-Outlook مما يتيح سرعة وصول المعلومة والتوزيع والتقليل من إستعمال الوثائق؛
 - لكل مستخدم كلمة مرور خاصة به يجب عليه تحديثها شهريا، تدرج في تسليم الهام لمن ينوبه في العمل. Back To Back.
 - الاعتماد على قاعدة البيانات الموحدة داخل الخادم Serveur، مما يتيح لكل مستخدم Utilisateur الوصول إلى الحيز الخاص بمجال عمله فقط؛
 - تخزين جميع الوثائق باستخدام ما يسمى بالأرشفة الإلكترونية، تحت مسؤولية مصلحة Doc Control؛
 - وجود مولد كهرباء حجم كبير خارج مبنى الإدارة، يشغل اتوماتيكي في حالة انقطاع الكهرباء؛
 - غرفة الخادم Serveur محمية بقفل إلكتروني خاص يقوم بتسجيل مدة البقاء داخل الغرفة ولا يفتح إلا للأشخاص المرخص لهم، أثناء أوقات العمل فقط، ومجهزة بمكيفين لضمان درجة الحرارة المناسبة داخل الغرفة، وأجهزة إنذار ضد الحرائق وأرتفاع درجة حرارة التوصيلات الكهربائية؛
 - تحتوي على خادمين يعملان بالتوازي وفي حالة حدوث عطب في أي منهما لا يشعر المستخدمين بذلك، وتوجه رسالة من الخادم قيد التشغيل إلى رئيس قسم الإعلام الآلي للتدخل؛
 - وجود خادم ثالث يقوم بمهمة التخزين الآلي للبيانات B de Stockage وذلك بالتوازي مع وحدة تخزين خارج الجزائر بمقر الشركة الأم في ساعات متأخرة من اليوم مبرمجة مسبقا؛
 - وجود أجهزة تخزين الكهرباء Onduleurs من الحجم الكبير خاصة بالخوادم؛
 - وجود جدار ناري عبارة عن جهاز Cisco يتم تسييره عن بعد من طرف شركة Cisco في فرنسا.
- كما توفر المؤسسات قوانين وقواعد حول امن نظام المعلومات وهي متاحة لجميع المستخدمين عبر الشبكة المحلية، وتشمل في:
- ✓ قواعد عامة:
- عدم الإفصاح عن المعلومات السرية المتعلقة بالعمل للأشخاص الغير مصرح لهم؛
 - يجب على الجميع أن يساهموا في الاستخدام الأمثل للنظام واحترام قواعد سلامة أجهزة تكنولوجيا المعلومات، والإبلاغ الفوري للمديرين في حال حدوث أي خلل في الأجهزة؛
 - المستخدمين مسؤولين عن طريقة استخدامهم للموارد الالكترونية خلال قيامهم بمهامهم داخل المؤسسة؛
 - يجب على المستخدمين الحفاظ على الموارد في مجال نشاطهم المهني، ويمنع الاستخدام الشخصي لوسائل الاتصال.
 - كما يمنع الموظفين من المشاركة في أي ظرف من الظروف في أي من الأنشطة التالية:
 - الحاق الضرر بموارد المؤسسة، وخاصة بما يتعلق بالنزاهة والحفاظ على البيانات الخاصة بالمؤسسة؛
 - التأثير السلبي على الصورة او السمعة الداخلية والخارجية للمؤسسة؛

- قراءة او فتح الملفات المشكوك فيها او التي تحتوي على الفيروسات؛
- استخدام موارد المؤسسة من طرف بعض المستخدمين لغرض منع الآخرين من استعمالها.
- ✓ اجراءات الامن الواجب احترامها من قبل المستخدمين:
- من اجل تنفيذ مهام المؤسسة على اكمل واحسن وجه، والحفاظ على نظام معلوماتها على المستخدمين احترام الاجراءات الامنية التالية و العمل بها:
- حماية الملفات السرية واسرار المؤسسة؛
- استخدام مضاد للفيروسات على أي ملف من مصدر خارجي للشركة؛
- عدم فتح او الرد على الرسائل الغير معروف مصدرها؛
- إيقاف البرنامج المستخدم وغلق جهاز الكمبيوتر الخاص بالطريقة الصحيحة؛
- عدم ترك نسخ الالكترونية (الاشرطة والاقراص الصلبة وغيرها) في اماكن مفتوحة وسهل الوصول اليها؛
- عدم ترك الوثائق في الفاكس والطابعات والآت النسخ؛
- يجب على الموظفين استخدام ادوات البريد الالكتروني من اجل العمل فقط؛
- الانترنت هي متاحة للمستخدمين ضمن الحدود المنصوص عليها في القانون الداخلي للمؤسسة فقط.
- ✓ قوانين خاصة بالاجهزة والبرمجيات:
- توفر المؤسسات مختلف الاجهزة الالكترونية والبرمجيات للمستخدمين التي تساهم في اداء مختلف الوظائف والانشطة متوافق مع القواعد والمتطلبات القانونية والتقنية التي حددتها الشركة لهذا الغرض، بالتالي فإن المستخدم ممنوع عليه تغيير هذه المعايير، بما في ذلك إضافة البرامج الغير معتمدة من طرف الشركة وهذا من اجل منع عمليات القرصنة محتملة.
- ان مستخدمي اجهزة الحاسوب المحمولة يلتزمون، بغض النظر لمكان تواجدهم، بحماية اجهزتهم بما في ذلك البيانات التي تحتوي عليها، وغير مسموح للمستخدمين اخراج الملفات التي لها قيمة استراتيجية للمؤسسة .
- كل اجهزة الحواسيب الخاصة والمحمولة، تحتوي على برامج مضادات الفيروسات حسب القاعدة العامة، وعلى الرغم من كل الاحتياطات المتخذة، فانها قد تتعرض للضرر جراء الفيروسات، وعليه فان البرامج او الملفات التي تتعرض للضرر يجب على المستخدم ايقافها على الفور واخبار المسؤول عن صيانة النظام بذلك من اجل اتخاذ التدابير اللازمة لمعالجة الضرر.
- كما تملك الشركة حق متابعة عمليات التفتيش والمراقبة بشكل نظامي وحسب ما ينص عليه القانون، ومعاقبة المخلين بالنظام.
- ثانيا: تحديد الاهداف العامة والخاصة للعملية، والمخاطر المحتملة:
- يقوم فريق التدقيق بتحديد الاهداف التي تسعى المؤسسة تحقيقها من هذه العملية، وكذلك تحديد المخاطر المحتملة والتي قد تخل بالنظام.
- 1- الاهداف العامة لعملية تدقيق نظام المعلومات: الاهداف العامة لمهمة تدقيق النظام هي تقييم درجة تطبيق وتسيير نظام الرقابة الداخلي والعمليات التشغيلية، وكذلك صياغة توصيات لتحسين جودة ادارة نظام المعلومات، وستسعى العملية الى التأكد من أن الأهداف العامة للرقابة الداخلية تحقق:
- أمن الأصول (المادية Hardware وغير المادية Software)؛
- الموثوقية وسلامة للمعلومات؛

- احترام القواعد والإجراءات؛

- كفاءة وفعالية نظام المعلومات ككل.

2- الأهداف الخاصة لعملية التدقيق : وتتضمن ما يلي:

1-2- سياسة أمن نظام المعلومات الالكتروني:

- التأكد من وجود سياسة أمن نظام المعلومات الالكتروني معلنة رسميا.

- التأكد من ان تنفيذ هذه السياسة يكون ضمن الاهداف التشغيلية.

2-2- التنظيم الخاص بنظام المعلومات الالكتروني:

- تقييم تنظيم ادارة نظام المعلومات الالكتروني، والتأكد من ادراج امن نظام المعلومات ضمن التنظيم.

- التحقق من وجود إجراءات ملائمة لضمان تطبيق أمن نظام المعلومات المعلومات.

- التأكد من توفر الموارد المادية والبشرية اللازمة لإدارة امن نظام المعلومات الالكتروني.

- التأكد من تطبيق عمليات التدقيق والفحص في مجال امن تكنولوجيا المعلومات.

3-2- إدارة الأصول والأمن المادي والبشري وتخزين البيانات:

- تأكد من أن أجهزة الحاسوب وأية معدات تخزين المعلومات تم تصنيفها وتركيبها بشكل صحيح، وفي مواقع مناسبة

لحمايتها من التهديدات المادية والبيئية (الرطوبة ومياه الأمطار، ...).

- التأكد من ان اجهزة الكمبيوتر والتيار الكهربائي موضوعة حسب المعايير، وان كل الاجهزة لها محولات الطاقة كهربائية.

- التأكد من ان الشبكة الكهربائية مطابقة وفقا للمعايير، و انه لا يوجد أية تهديدات لعمليات تنصيب اجهزة الحاسب.

- التأكد من ان شبكات المياه الصناعية و الصالحة للشرب، لا تشكل اية تهديدات للتجهيزات الالكترونية.

- التأكد من ان اي تهديد اخر مثل الحرائق، تم تحديدها و وضع التدابير اللازمة لها.

4-2- الشبكات الالكترونية:

- التأكد من عمليات التطوير الرسمي للشبكة الالكترونية، وتوفير مختلف التسهيلات لتدخل في عمليات التطوير.

- التأكد من ان امن الشبكة الالكترونية مدعومة من طرف الموارد المادية والبشرية في المؤسسة.

- التأكد من ان الشبكة الالكترونية محمية ضد مختلف التهديدات وذلك بتوفير مختلف التطبيقات اللازمة للحماية.

5-2- السلامة المتعلقة بالموارد البشري:

- التأكد من تنفيذ وتطبيق الاجراءات والتدابير الاحتياطية اللازمة ضد مخاطر سرقة البيانات.

- التحقق من ان كل الموظفين المخول لهم الوصول الى البيانات لديهم كلمة سر خاصة بهم.

6-2- تطوير وصيانة نظم المعلومات الالكتروني:

- التأكد من ان مخططات قاعدة البيانات متوفرة وتقييم مدى سلامتها.

- التأكد من ان مصادر البيانات مشفرة من طرف مطوري البرمجة، والتأكد من انها لا تحتوي على شيفرات خبيثة.

7-2- الادارة التشغيلية:

- التأكد من تحديد مصادر المخاطر (الاختراقات والهجمات، والبرمجيات الخبيثة).

- التأكد من عمليات تقييم المخاطر (من حيث التأثير واحتمال حدوثها، والطبيعة، والنشاط، ...).

- تقييم تدابير الرقابة والحماية المنفذة.

- القدرة على مراقبة الدخول او الوصول الى التطبيقات (تطبيقات الموارد البشرية، الاجور، المحاسبة، ...).

- التأكد من ان برامج مضادات الفيروسات مرخصة ومثبتة على مستوى الاجهزة الالكترونية ويتم تحديثها.

8-2- ادارة الحوادث المتعلقة بامن نظام المعلومات، واستمرارية الاعمال.

- التحقق من وجود وتنفيذ إجراءات إدارة الحوادث.
- معرفة ما اذا كانت خطة إدارة حوادث نظم المعلومات الالكترونية تضمن استمرارية العمل.

9-2-طريقة عمل البرنامج:

- التأكد من ان البيانات المدخلة الى البرنامج تطابق الوثائق الورقية.
- التأكد من طريقة عمل التطبيقات (المعالجة) وذلك عن طريق استخدام برنامج اخر للتأكد من النتائج.
- التأكد من صحة المخرجات ومطابقتها لعملية المعالجة.

3- جدول المخاطر:

يتم تحديد مسارات عملية تدقيق النظام ونقاط الفحص بالاعتماد على الأهداف العامة والخاصة للعملية، وعليه يتم تحديد المخاطر المحتملة والمتعلقة بنظام المعلومات والتي تشمل الأهداف الخاصة للعملية، وفيما يلي الجدول يوضح أهم مسارات عملية التدقيق والمخاطر المحتملة:

الجدول رقم (05) : جدول المخاطر المتعلقة بنظام المعلومات.

مسارات التدقيق ونقاط الفحص	المخاطر المترتبة
سياسة امن نظام المعلومات	-السياسات الرسمية لامن نظام المعلومات - اهداف، ومهام، ومسؤوليات (DINTIC) و (IT) من امن نظام المعلومات الالكتروني.
التنظيم الخاص بنظام المعلومات الالكتروني.	- تنظيم ومهام، مسؤوليات قسم نظام المعلومات الالكتروني. - الاجراءات، والقوانين، والزامية التنفيذ. - الموارد البشرية والمادية المخصصة لأمن نظام المعلومات الالكتروني. - عمليات التدقيق والفحص المنجزة في مجال أمن نظام المعلومات الالكتروني.
إدارة الأصول، والأمن المادي والبشري وتخزين البيانات	-قائمة المعدات والاجهزة الالكترونية. - المكاتب التقنية، ورشات العمل وغرفة الاجهزة الالكترونية. - معدات الطاقة والمحولات الكهربائية. - شبكة امدادات المياه التي قد تشكل خطرا على الاجهزة الالكترونية. - الحماية ضد الحرائق.
الشبكات الالكترونية	-بنية شبكة نظام المعلومات الالكتروني. -الموارد البشرية والمادية المخصصة لأمن الشبكات الالكترونية.
بالمورد البشري المتعلقة السلامة	-وسائل أمن بيانات الكمبيوتر. -التعليمات البرمجية لقواعد استخدام نظام المعلومات الالكتروني.
	-التركيب غير سليم للاجهزة الالكترونية -نقص الموصلات بين الحواسيب وشبكة الكهرباء -عدم كفاية المحولات الكهربائية. -الشبكة الالكترونية منفذة خارج المعايير، حيث انها تشكل تهديدا للاجهزة الالكترونية. -خطر تسرب مياه، والرطوبة. -معدات الحماية ضد الحرائق غير كافية.
	-غياب بنية الشبكة. -غياب او عدم كفاية الموارد البشرية والمادية مخصصة لإدارة أمن الشبكات.
	-خطر اختلاس البيانات. -خطر إفشاء السر المني. -اخطار التحريف الخطء والمتعمد - خطر الحذف الخطء او المتعمد

تطوير وصيانة نظم المعلومات	- دراسة (تصميم) مشروع تطبيقات الحاسوب. -مخططات قواعد البيانات. -شفرة مصادر البيانات الصادرة عن تطبيقات الحاسب.	-عدم وجود دراسات تصميمات لمشاريع تطبيقات الحاسوب. -عدم وجود مخططات لقواعد البيانات. -شيفرات امنية ضعيفة وضعت للبيانات الصادرة عن مختلف تطبيقات الحاسب.
الادارة التشغيلية.	-الإجراءات لتحديد مخاطر نظام المعلومات الالكتروني (الاختراقات والهجمات، والبرمجيات الخبيثة). -تدابير الرقابة والحماية ضد مخاطر نظام المعلومات الالكتروني. -إجراءات الترخيص للوصول إلى التطبيقات وقواعد البيانات -قائمة مضادات الفيروسات التي تستخدمها مختلف إدارات الشركة.	-عدم وجود الإجراءات العملية التي تحدد مخاطر نظام المعلومات الالكتروني. -عدم معرفة مخاطر نظام المعلومات الالكتروني وتأثيرها. -عدم كفاية التدابير للمراقبة والحماية ضد مخاطر نظام المعلومات الالكتروني. -ال فشل في إدارة الوصول إلى التطبيقات وقواعد البيانات. - عدم استخدام مضادات الفيروسات او غياب عمليات تحديثها.
ادارة الحوادث امن المعلومات، واستمرارية الأعمال	- القواعد والاجراءات المتعلقة بادارة حوادث او مخاطر نظام المعلومات. - مخطط ادارة حوادث او مخاطر نظام المعلومات الالكتروني.	-عدم وجود القواعد والإجراءات المتعلقة بادارة حوادث او مخاطر نظام المعلومات. -غياب مخطط ادارة حوادث او مخاطر نظام المعلومات الالكتروني.
طريقة عمل البرنامج	-الوثائق الورقية المعتمدة في اذخال البيانات. - طريقة عمل التطبيقات المختلفة. -مخرجات النظام.	-عدم مطابقة المدخلات للوثائق الورقية. -طريقة المعالجة تؤدي الى نتائج غير صحيحة. -عدم مطابقة المخرجات لعملية المعالجة.

المصدر: من اعداد الباحثين اعتمادا على نتائج المقابلة والملاحظة.

ثالثا. نقاط الضعف:

فيما يلي تحديد نقاط الضعف المسخرجة من دراسة وتحليل المخاطر التي تم تحديدها في المرحلة الاولى، ومعرفة اسبابها:

رقم1: عدم وضع الملفات الرئيسة في الأرشيف على مستوى بعض المديرية؛

رقم2: إلغاء تثبيت مضادات الفيروسات من قبل المستخدمين؛

رقم3: مخاطر الشبكة الكهربائية على الأجهزة الالكترونية؛

رقم4: الخطر المادي على غرفة الأجهزة الالكترونية؛

رقم5: عدم التمكن من السيطرة على عملية سرقة البيانات من قبل الموظفين؛

رقم6: تأخير في تنفيذ عقد الصيانة لنظام مكافحة الحرائق في غرفة الأجهزة الالكترونية؛

رقم7: ميثاق امن نظام المعلومات غير معلن عنه اي غير متاح لجميع الموظفين الذين يستخدمون النظام.

رابعا: النتيجة: بها يتم اعداد التقرير النهائي لعملية التدقيق، والذي يتضمن نتيجة العملية وإبداء رأي المدقق الداخلي حول كفاءة وفعالية نظام المعلومات الالكتروني، ويتم فيه تحديد كافة النقاط المهمة التي مرت بها العملية وتقديم توصيات حول نقاط الضعف، وفي الاخير عقد اجتماع مع رئيس المديرية من اجل اطلاعه على النتائج النهائية، وتقديم نسخة من التقرير الى المدير العام ونسخة الى المديرية، ونسخة تحتفظ بها مديرية التدقيق.

الخلاصة:

ان من اهم عوامل نجاح او فعالية نظم المعلومات في المؤسسة هو الاستغلال الامثل لموارد النظام (المادية، غير مادية، بشرية)، وعليه حاولنا في دراستنا تقييم كفاءة نظام المعلومات بمؤسسة عومية مقارنة بمؤسسة شراكة (اجنبية-وطنية) لمعرفة اهم النقاط التي تحول دون الاستغلال الأمثل للنظام، تبين وجود قصور كبير في المؤسسة ENAGEO، يعزى بالدرجة الأولى إلى إهمال المورد البشري، و غياب الصرامة في تنفيذ الإجراءات، والإحساس بالمسؤولية لدى الجميع، وبناء عليه توصلنا إلى النتائج

التالية:

1. تمتلك المؤسساتين موارد متطورة من أجهزة الحاسوب وبرامج وشبكات؛
2. الإجراءات والقواعد والتنظيمات الخاصة المديرية تكنولوجيا المعلومات بالمؤسسة الوطنية للجيوفيزياء تتناسب مع المهام الموكلة إلیها من قبل الإدارة العليا، إتقان جيد للأنشطة التنفيذية من قبل موظفي المديرية، والسعي إلى التحسين؛
3. إجراءات إعداد وتحديث نظام المعلومات لالكتروني تغطي معظم الأنشطة في كلا المؤسساتين؛
4. لا تقوم الادارة العليا للمؤسسة الوطنية للجيوفيزياء بالأخذ بعين الاعتبار لنتائج عملية تدقيق نظام المعلومات الموجودة في التقرير، وذلك باتخاذ الإجراءات الضرورية لتدارك مختلف المشاكل الموجودة داخل نظام المعلومات، والسيطرة عليها في الوقت المناسب.
5. الاعتماد على المعيار الدولي ISO 9001 في انجاز وتطوير التطبيقات من قبل بالمؤسسة الوطنية للجيوفيزياء وكذا مؤسسة HESS؛
6. يتمثل الهدف الرئيسي لعملية تدقيق نظام المعلومات في المؤسساتين هو تقييم النظام من حيث معرفة مدى كفاءته وفاعليته بالمؤسسة لكن بالنسبة للمؤسسة الوطنية للجيوفيزياء لا يؤخذ بعين الاعتبار تقارير المدقق، عكس مؤسسة HESS التي تسعى إلى تطبيق كل توصيات المدقق (التوصيات المتعلقة بنظم المعلومات)؛
7. نظم المعلومات الالكترونية بالمؤسساتين تحقق الأهداف المرجوة الا انها لا تتصف بالكفاءة اللازمة في المؤسسة Enageo، اي لا يتم الاستغلال الجيد لموارد نظام المعلومات في تحقيق الاهداف؛
8. تعاني المؤسسة الوطنية للجيوفيزياء من عدم امكانيتهما من استغلال كل البرامج الموجهة للإدارة؛
9. تعاني مؤسسة HESS من خطر سرقة و الاطلاع على المعلومات وهذا لانها تلجأ إلى الصيانة الخارجية للعتاد؛
10. يتميز العنصر البشري في المؤسسة الوطنية للجيوفيزياء بشدة المقاومة لأي تغيير يتعلق بنظم المعلومات و عليه يعيق تطوير النظام في ظل غياب ادارة التغيير في المؤسسة؛
11. يتميز العنصر البشري في مؤسسة HESS بمرونة عالية مع التغيير عكس المؤسسة الوطنية؛
12. لدى المؤسسة الوطنية للجيوفيزياء فريق مسير لنظام المعلومات في المؤسسة شاب و كفؤ، كما لمسنا ان لديهم حس ابداعي عالي.

بناء على النتائج السابقة نحاول ان نقدم التوصيات الآتية:

1- بالنسبة للمؤسسة الوطنية للجيوفيزياء:

- إيقاف ميزة الالغاء للبرامج بالنسبة للمستعملين وخاصتها الغاء تشغيل مضادات الفيروسات؛
- اعداد مدونة لقواعد السلوك لاستخدام نظام المعلومات الالكتروني وتنفيذها؛
- اتخاذ التدابير اللازمة للحد من خطر اختلاس البيانات وهذا بمنع استخدام USB، CD، الابدخيس من مديرية تكنولوجيا المعلومات والاتصال؛
- تقييم الاحتياجات اللازمة لمختلف البيانات بالنسبة للمديريات وايجاد الحلول لها؛

- اتخاذ الاجراءات والتدابير اللازمة للوقاية في حالة تسرب المياه؛
- اعطاء اهمية اكثر للشبكة الكهربائية وتحويل خزائن الكهرباء من داخل مديرية تكنولوجيا المعلومات و الاتصال وإضافة مولد كهرباء؛
- الزامية احترام وتنفيذ لعقود صيانة نظام الوقاية من الحرائق، واسناد المسؤولية لجهة محددة للمتابعة؛
- الاعلان والزامية تنفيذ الميثاق المتعلق بأمن نظام المعلومات على مستوى كل المديرية، ومعاقبة المخالفين لذلك وإرسال دوري للتذكير في بريد النظام كل شهر مثلا؛
- إدراج إدارة امن نظام المعلومات ضمن مستوى عالى في الادارة لاعطائها قوة اكبر لتدعيم تطوير النظام الالكتروني؛
- عزل الخوادم les Serveurs عن باقي المعدات، لانه ليس كل المرخص لهم بدخول المديرية مرخص لهم لمسه؛
- الاهتمام بفريق المهندسين المكلفين بتطوير نظام المعلومات من حيث التحفيز.

2- بالنسبة للمؤسسة الاجنبية Hess:

- إعداد البطاقات المهنية داخل المؤسسة وذلك لتقليل زمن إعداد البطاقة الإلكترونية عند ضياعها، ومنع تسرب نسخ من البطاقات لأشخاص غير مرخص لهم؛
- إضافة منصب لصيانة العتاد الخاص بنظام المعلومات داخل المؤسسة وذلك لضمان سرية المعلومات؛
- تعديل في الأقفال الإلكترونية بحيث يمكن فتحها يدوياً في حالة الضرورة؛
- منع ارسال الملفات المرفقة ذات الحجم الكبير، والاكتفاء بارسال مكان تواجدها link، لانها مخزنة في الخادم اصلا؛
- اعتماد وفرض البريد الإلكتروني على المتعاملين (الموردين المحليين) في النظام مباشرة، واعتماده كدليل اثبات في التعاملات والفوترة الخارجية، وهذا بسبب غرامات التأخير في الدفع.

الاحالات والمراجع:

¹ رجم خالد، تقييم اثر نظام معلومات الموارد البشرية على استراتيجيات الموارد البشرية في قطاع النفط، اطروحة دكتوراه، غ منشورة، جامعة ورقلة، 2017، ص 47.

² Robert Longeon, Jean-Luc, Guide de la sécurité des systèmes d'information, Paris, France, 2009, P10

³ Ayari amani " audit de sécurité du système informatique de MTIC " mémoire de mastere professionnel « Nouvelles Technologies des Télécommunications et Réseaux » Université virtuelle de tunis, 2014, p 14.

⁴ علوطي لمن "تحديات الامن الالكتروني في المؤسسة"، مجلة الابحاث الاقتصادية و الادارية- العدد السادس ديسمبر 2009، جامعة المدية، ص 169.

⁵ Robert Longeon, OPCIT, P12

⁶ Micelle Gillet " Management Des Systèmes D Information, Manuel Et Applications DSCG 5 " 2^{ème} édition DUNOD; paris, 2010, P 375

⁷ Ayari amani " audit de sécurité du système informatique de MTIC " mémoire de mastere professionnel « Nouvelles Technologies des Télécommunications et Réseaux » Université virtuelle de tunis, 2014.

⁸ رجم خالد، مراجعة نظام المعلومات، محاضرات ضمن مقياس مراقبة و مراجعة نظام المعلومات، اولى ماستر تدقيق، جامعة ورقلة، ص 40، 2017.

⁹ اطلع عليه يوم 05-06-2017 http://www.accdiscussion.com/t12332.

¹⁰ رشا حمادة "أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الالكترونية في زيادة موثوقية المعلومات المحاسبية" جامعة دمشق مجلة جامعة دمشق للعلوم الاقتصادية والقانونية -المجلد - 26 العدد الأول 2010 -ص 318.

¹¹ زياد عبد الحليم الذبيبة "نظم المعلومات في الرقابة و التدقيق" دار الميسرة للنشر و التوزيع و الطباعة عمان الاردن. الطبعة الاولى 2011 ص 35.

¹² متاح على الموقع : http://islamfin.go-forum.net/t1220-topic تم الإطلاع عليه يوم 11-05-2017.