أثر ممارسة اليقظة عبر الانترنيت على درجة حماية وأمن المعلومات في المؤسسات الجزائرية

The effect of practicing internet monitoring on the degree of information protection and security in Algerian institutions

جيلالي شفيق*[1]، لحشم قسمية[2]

[1]جامعة البليدة 2، الجزائر، djiali.chafik@gmail.com

[2] جامعة البليدة 2، الجزائر، kasmia.lahchem@gmail.com

تاريخ الاستلام:2022/04/14 تاريخ القبول:2022/05/16 تاريخ النشر :2022/06/15

ملخص:

تهدف هذه الدراسة إلى إبراز طبيعة العلاقة التأثيرية بين ممارسة اليقظة عبر الإنترنيت في المؤسسات وبين مستوى حماية وأمن المعلومات لديها، بالتطبيق على عينة من المؤسسات الجزائرية، وقد تم إجراء استقصاء ميداني على عينة مكونة من 30 مؤسسة تنتمي إلى مختلف القطاعات الاقتصادية . وباستخدام أساليب الاختبار الإحصائية المناسبة توصلت الدراسة إلى إثبات وجود أثر ذو دلالة إحصائية بين اليقظة على الإنترنيت ومستوى أمن وحماية المعلومات في المؤسسات محل الدراسة. وبناء على نتائج الدراسة تم تقديم عدد من التوصيات والمقترحات من بينها ضرورة سياسة متكامل لاستغلال الإنترنيت في جمع المعلومات المفيدة من خلال اليقظة، مع تخصيص الوقت والأموال اللازمة لتطوير الأساليب والأدوات التي تخدم هذا الغرض، كذلك ضرورة تدريب الموظفين في كافة المستويات على طرق وتقنيات جمع وحماية المعلومات المفيدة المتعلقة بمجال نشاط المؤسسة، وضرورة توعيتهم بأهمية الالتزام بقواعد أمن وسرية المعلومات.

الكلمات المفتاحية: يقظة، يقظة عبر إنترنيت، حماية وأمن معلومات.

ترميز JEL : M15, L86, G14

Abstract:

This research paper aims to study the influence relationship between the practice of internet monitoring in enterprises and the level of protection and information security system those enterprises, therefore questionnaire was distributed to a sample of 30 Algerian enterprises belonging to various economic sectors. The study concluded that there is a statistically significant effect between internet monitoring and the level of information security and protection in the enterprises. Recommendations were presented, including the need for an integrated policy to exploit the Internet in collecting useful information through monitoring, as well as the need to train employees at all levels on methods and techniques for collecting and protecting useful information related to the enterprises' field of activity, and the need to sensitize them about the importance of adhering to the rules of information security and confidentiality.

Keywords: Monitoring, internet monitoring, Information security and protection.

JEL Classification Codes: G14 , L86, M15

* **المؤلف المرسل**

1. مقدمة:

إنّ نجاح أي مؤسسة اليوم أصبح يعتمد على قدرتها في الاستجابة والتكيف مع ما يحدث في بيئتها ، بهدف البقاء و الاستمرار في السوق، نتيجة للتطورات الحاصلة في تلك البيئة سواء في حجم المنافسة واشتدادها و عولمة الأسواق وتطورها بالإضافة إلى زيادة التركيز على الجودة و الابتكار و التوجه نحو المستهلك، وكذا تعقد النشاط التسويقي ،مما حتّم على المؤسسة أن تكون في حالة ترصد دائم ومستمر لكل المتغيرات المحددة لأنشطتها المختلفة، وبالتالي تجد المؤسسات نفسها مضطرة إلى البحث عن الحلول التي يمكن أن تساعدها في تحديد المعلومات ذات الصلة، وبهدف تحسين القدرة على توقع الفرص والتهديدات التي تحيط بها ، ولا يتسنى لها ذلك إلاّ عبر الاستعانة بالأدوات والوسائل التي تساعد على التحكم في الكم الهائل من المعلومات التي تصف كل تلك المتغيرات.

في ظل ما سبق، ظهرت الحاجة إلى التكامل في استخدام المعلومات نتيجة لتعقد وكبر حجم الأنشطة في المؤسسات المعاصرة، ففي بعض الحالات قد تستطيع المؤسسة الحصول على جميع المعلومات المعتمد في اتخاذ القرارات غير أنه في حالات أخرى لا يستطيع الحصول عليها مما يؤدي بها إلى اتخاذ قرارات متذبذبة تتميز بعدم التأكد، فتجنبا لمثل هذه الحالات يترتب على المؤسسة تبني اليقظة كأداة تقدم المعلومات الصحيحة الدقيقة الشاملة والمناسبة وفي الوقت المناسب لاتخاذ قرارات ذات كفاءة وفعالية.

من ناحية أخرى أصبح الإنترنت أهم قناة لاتصال المؤسسة مع بيئتها لما تتمتع به من قدر هائل من المعلومات التي يحتمل أن تكون مفيدة للمؤسسة ، فهي تتيح الفرصة للمؤسسات للوصول إلى مصادر معلومات جديدة وبأقل تكلفة عن الطرق التقليدية، وازدادت أهمية هذا الوسيلة مع تطور تطبيقات الاقتصاد الافتراضي وما يتيحه من إمكانية لاستغلالها لممارسة الأنشطة التسويقية بالدرجة الأولى، فالإنترنت يسمح بتطبيق الأدوات والإجراءات الفعالة للبحث وجمع المعلومات ومعالجتها ونشرها، حيث تعد الإنترنيت مصدرًا غنيًا للمعلومات التي يمكن أن تساعد في الترقب شريطة استغلال الوسائل المناسبة. وتعتبر أحد اليقظة أهم هذه الوسائل والأدوات المقترحة على المؤسسات لاستغلال الإنترنيت في هذا الصدد.

هذا ورغم الفائدة التي تعود على المؤسسة من استغلال الإنترنيت لجمع المعلومات بواسطة اليقظة، إلا أن هذا النشاط لا يخلو من المخاطر التي قد تمس تلك المؤسسة، من حيث إمكانية تعرض المعلومات التي تجمعها لمخاطر السرقة أو الإتلاف والقرصنة. فالمؤسسات مطالبة بأن تحافظ على مستوى حماية للموارد غير الملموسة من المعلومات المستخدمة في اتخاذ القرارات على مختلف المستويات، وذلك عبر بناء نظام أمني يحافظ على مستوى الأمان المفترض، واتخاذ تدابير وقائية لرعاية أمن المعلومات بشكل فعال. فمن الضروري تنفيذ بعض الضمانات التي تؤدي إلى تقليل مخاطر هذا النوع من التهديدات، والرعاية المناسبة لأمن وحماية المعلومات.

لقد اتجه فكرنا إلى محاولة الجمع بين الأفكار والمفاهيم التي نراها لازمة لتقديم الموضوع في شكل يسهم في بناء الإطار الشامل لموضوع بحثنا، وعلى أسس متوازنة، لأجل ذلك خصصنا هذا العمل لعرض أحد أهم المتطلبات اللازمة لتطبيق اليقظة عبر الإنترنيت في المؤسسات الاقتصادية لما لها من خصائص تسييرية من

جهة، ومن جهة أخرى اقتراح الوسائل والإجراءات الكفيلة بتوفير الحماية والأمن للمعلومات التي تتحصل عليها المؤسسة جراء استغلالها لهذه الوسيلة.

لهذا كانت دراستنا من أجل الإجابة على هذا التساؤل: **هل يؤثر تطبيق المؤسسات لليقظة عبر الإنترنيت على مستوى حماية وأمن المعلومات لديها؟**

والتي يندرج تحتها الأسئلة التالية:

- كيف يمكن وضع حيز التنفيذ نظام لليقظة يساعد على جمع المعلومات المفيدة؟
- هل تعتمد المؤسسات محل الدراسة على ممارسة اليقظة عبر الانترنيت في جمع المعلومات؟ وما هو واقع حماية وأمن المعلومات لديها؟
- هل هناك علاقة بين مستوى حماية وأمن المعلومات وبين اليقظة على الانترنيت لدى المؤسسات محل الدراسة؟

وقد تم صياغة الفرضيات التالية للدراسة:

الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية في تطبيق اليقظة على الانترنيت في المؤسسات محل الدراسة تعود لامتلاكها سياسة محددة ومنظمة لجمع المعلومات على الانترنيت"

الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية في مستوى أمن وحماية المعلومات في المؤسسات محل الدراسة تعود لامتلاكها سياسة محددة ومنظمة لجمع المعلومات على الانترنيت "

الفرضية الثالثة" "لا يوجد أثر ذو دلالة إحصائية بين اليقظة على الانترنيت ومستوى أمن وحماية المعلومات في المؤسسات محل الدراسة "

هذا وقد لقد تعددت الدراسات التي تناولت موضوع اليقظة عبر الإنترنيت وكذا أمن وحماية المعلومات في المؤسسة، لكن مع قلة الدراسات التي ربطت بين المتغيرين. ومن أهم الدراسات السابقة، نذكر:

- **دراسة بوداود** (بوداود، 2019)

بعنوان (دور الانترنت في إرساء اليقظة الإستراتيجية بمؤسسة اتصالات الجزائر– وهران)،هدفت هذه الدراسة إلى معرفة مساهمة الانترنت في إرساء اليقظة الإستراتيجية داخل المؤسسة الاقتصادية الجزائرية، وتحقيقا لغايات الدراسة، تم الاعتماد على استبيان موجه لموظفي الإدارة العامة في شركة اتصالات الجزائر بوهران.وقد تم التوصل إلى وجود علاقة ارتباط بين الانترنت واليقظة الإستراتيجية بما يجعل لها دور مميز وأساسي لا يمكن الاستغناء عنه في إرسائها داخل مؤسسة، وكذلك أن للانترنيت بصفة خاصة وتكنولوجيات الإعلام والاتصال بصفة عامة اثر ايجابي على اليقظة الإستراتيجية لمؤسسة اتصالات الجزائر لولاية وهران، ودور فعال لا يمكن قيام المؤسسة المدروسة دونه حيث يشكل دعامة قوية في بناء نظام اليقظة الإستراتيجية ونجاحها في جميع مراحلها والتوصل إلى نتائج أفضل مما يضمن استمرارية المؤسسة ومواكبة التطورات.

- **دراسة Żywiołek** (Żywiołek, 2018,July 31)

هدفت هذه الدراسة إلى تحديد أسباب مراقبة تدفق المعلومات في المؤسسة التي تمارس اليقظة، وأن تحديد مصادر المعلومات يسهل عملية إدارتها، ويزيد من قدرة الأفراد على معالجة المعلومات وتجنب الحوادث المرتبطة بأمن المعلومات. كما أن تنفيذ أساليب إدارة المعلومات يسهل مراقبة حالة أمن المعلومات. وقد توصلت الدراسة إلى أنه من الضروري اتخاذ تدابير وقائية من أجل أن تكون المؤسسة أكثر ذكاءً قبل الأذى، وتهتم بشكل فعال بأمن المعلومات داخلها. كما أنه من الضروري تنفيذ بعض الضمانات التي تؤدي إلى تقليل خطر التهديدات الناتجة عن استخدام الانترنيت ، لأنها في الغالب ناتجة عن فعل متعمد للموظف ، وليس عن جهله أو بسبب حادث. يجب الحفاظ على سياسة أمن المعلومات، ويجب أن تكون هناك إستراتيجية رسمية وخاضعة للإشراف المستمر، افتراض هذه الإستراتيجية هو التعرف على عمليات اليقظة وتصنيفها وفحص تدفق المعلومات. كما يمكن تنفيذ إستراتيجية أمن المعلومات بفضل استخدام أساليب إدارة المعلومات.

- **دراسة ولد عابد و علواطي** (ولد عابد و علواطي، 2017)

هدفت هذه الدراسة إلى تقديم نموذج مقترح لتطبيق آليات اليقظة الإستراتيجية بالمؤسسات الاقتصادية الجزائرية، مع إسقاط النموذج على مؤسسة الإسمنت بالشلف، وذلك من خلال التعرف على كيفية عمل النظام المقترح لليقظة الإستراتيجية و ما يمكن أن تقدمه من ميزات لمؤسسة وكذا معرفة مختلف الوظائف وعمليات هذا الجهاز وكذا حركية المعلومات فيه وكيفية مساهمته في إيجاد ميزات تنافسية وتحسين القرارات الإستراتيجية بالمؤسسة.أما عن أهم مخرجات الدراسة فتمثلت في ضرورة تبني المؤسسات الجزائرية لثقافة اليقظة الإستراتيجية لما لها من أهمية كبيرة خاصة بعد انفتاح الأسواق الجزائرية أمام المنافسة الدولية، وإلى استحداث مصلحة خاصة على مستوى المؤسسة تختص بجمع المعلومات عن مختلف العناصر البيئية؛ بمعنى إيجاد خلية لليقظة الإستراتيجية يتم من خلالها تنظيم وتدعيم، جهود الأفراد في البحث عن المعلومات الهامة، بحيث تصبح تؤدى في شكل نشاطات تعنى حقيقة باليقظة على البيئة الخارجية.

- **دراسة قدي ونحاسية** (قدي و نحاسية، 2014)

هدفت الدراسة إلى تقديم تصنيف حسب الفئات لأدوات البحث عن المعلومات عبر الويب، الضرورية لتنفيذ سيرورة اليقظة الاسترتيجية.حيث تتضاعف المعلومات على الويب بمعدل غير عادي، كما أن الوسائل التي يتم من خلالها نقل المعلومات عبر الويب هي في تزايد أيضا. وفي هذا السياق، تجد المؤسسات نفسها أمام التحدي المتمثل في الحمل الزائد للمعلومات، حيث يصعب عليها أكثر فأكثر معرفة إذا كانت تلك المعلومات التي تم الحصول عليها هي معلومات ملائمة أم لا. لهذا، تحتاج المؤسسة إلى أن تتجهَّز بنظام اليقظة الاستراتيجية الذي يسمح لها بجمع، تخزين، تحليل ونشر المعلومات لأغراض استراتيجيـة. ويعتبر البحث عن المعلومات عبر شبكة الويب، الاختيار الأمثل للمؤسسة، من منطلق أنه يُمَّكِنها من الحصول وبسرعة على المعلومات التي تحتاجها. ومن أجل ذلك، يجب على المؤسسة أن تستعمل عدد معين من الأدوات التي ستساعدها لإتمام هذه المهمة.

- **دراسة Dempsey** (Dempsey, et al., 2011)

الغرض من هذه الدراسة هو مساعدة المؤسسات في تطوير إستراتيجية مراقبة مستمرة وتنفيذ برنامج يقظة مستمر يوفر رؤية حول وضعية المؤسسة، والوعي بنقاط الضعف والتهديدات التي تواجهها ، وإبراز فعالية الضوابط الأمنية التي يتم اعتمادها في حماية الأصول غير المادية للمؤسسة.مع التأكيد على ضرورة توفير الضمانات بصفة مستمرة بأن الضوابط الأمنية المخطط لها والمنفذة تتماشى مع المخاطر التي يتم تحملها، بالإضافة إلى المعلومات اللازمة للاستجابة للمخاطر في الوقت المناسب.وقد توصلت الدراسة إلى أن الضوابط الأمنية في المؤسسات غير كافية.وبالتالي ضرورة تطوير إستراتيجية لليقظة بصفة مستمرة مع التأكد من أنها تدعم أنشطة المؤسسة بشكل كافٍ، مع العمل على اتخاذ التدابير اللازمة للحفاظ على الوضع الأمني للمؤسسة أو تحسينه.

-ما يميز الدراسة الحالية عن الدراسات السابقة.

تقترح الدراسة الحالية إطارا لدراسة ممارسة اليقظة عبر الانترنيت، نظرا لما توفره هذه الأخيرة من مصادر هائلة للمعلومات، وبتكلفة منخفضة، فضلا عن ربط هذه الممارسة مع ضرورة توفير شروط الأمن والحماية للمعلومات التي تجمعها المؤسسة. من جهة أخرى وحسب اطلاع الباحثين فإن أيا من الدراسات السابقة لم تدرس العلاقة بين اليقظة عبر الانترنيت وأمن المعلومات بالتطبيق على عينة من المؤسسات الجزائرية ، وهي الإضافة الرئيسية التي يقترحها الباحثين من خلال استبيان مصمم خصيصا لذلك، وبالتالي تقديم جملة من الاقتراحات التي تزيد من فعالية ممارسة اليقظة عبر الانترنيت، وزيادة كفاءة وفعالية الإجراءات المتخذة لحماية معلومات المؤسسة كأصل غير ملموس يستخدم في اتخاذ القرارات على مختلف المستويات الإدارية في المؤسسة.

حيث نهدف عبر هذه الدراسة إلى اقتراح استخدام جديد للإنترنت للمساعدة في توليد معلومات مفيدة من خلال تطبيق اليقظة لمديري المؤسسات الراغبين في ممارسة الإدارة الإستباقية، مع ضمان مستوى أمن وحماية للمعلومات التي يتم جمعها دون التعرض إلى مختلف المخاطر والتهديدات التي يمكن أن تلحق الضرر بهذا المورد الثمين.

2. الإطار النظري للدراسة:

1.2. اليقظة: مفهومها وأشكالها.

تستعمل كلمة اليقظة للإشارة إلى الرغبة للاستمرار في حالة من الوعي لحراسة ومراقبة شيء ما والحفاظ عليه.أما في مجال الأعمال فهي تشير إلى الوظيفة التي ترتبط بتسيير موارد المعلومات لتجعل المؤسسة أكثر ذكاء وتنافسية (Bergeron, 1995, p. 18). ويمكن تعريف اليقظة بأنها العملية الجماعية المستمرة، والتي يقوم بها مجموعة من الأفراد بطريقة تطوعية، فيتتبعون ويتعقبون ومن ثم يستخدمون المعلومات المتوقعة التي تخص التغيرات التي من المحتمل أن تحدث في البيئة الخارجية للمؤسسة، وذلك بهدف إنشاء فرص الأعمال وتقليل المخاطر وعدم التأكد بصفة عامة (Janissek-Muniz, Freitas, & Lesca, 2006, p. 20) ، فاليقظة يمكن تشبيهها برادار السفينة كونها تساعد على استباق الأحداث ومواجهتها قبل فوات الأوان. أي أن اليقظة عبارة عن

عملية معلوماتية تبحث المؤسسة بواسطتها على توقع إشارات الإنذار بهدف خلق فرص السوق وتقليص الأخطار المرتبطة بعدم التأكد(Ayachi, 2007, pp. 52-53) .

ويمكن لليقظة أن تتخذ ثلاث أشكال رئيسة في المؤسسة هي:

-اليقظة السلبية أو مستوى المسح: تمثل أولى مستويات اليقظة وتكمن مهمتها في تتبع متغيرات بيئة المؤسسة دون تحديد مؤشرات معينة تبحث عنها، في هذه الحالة تكون البيانات المجمعة ذات قيمة مضافة ضعيفة بسبب التركيز على المعلومات المنشورة سابقا أو المعلومات البيضاء، وتتعلق بمجمل وظائف المؤسسة ولا ترتبط بأهداف محددة مسبقا، فالمؤسسة يمكن أن تجد نفسها غارقة في كم من التفاصيل التي قد تشكل خطر يحد من قدرتها على اتخاذ القرارات الجيدة.مما يدفعها إلى البحث عن أساليب أخرى لتسيير المعلومة.

-اليقظة النشطة أو مستوى المراقبة والتحذير: في هذا المستوى تصبح مهمة اليقظة فتح منافذ لملاحظة البيئة والبحث عن معلومات جد دقيقة ومحددة. وهذا النوع يعتمد على مصادر المعلومات الرمادية وعلى تطوير ردة الفعل الاتصالية للموظفين في مجال مصادر المعلومات، وقد يتم الاستعانة هذه الحالة بلوحات قيادة تسمح بإرسال إشارات إنذار عند رصد بعض نقاط الخلل في بيئة المؤسسة.

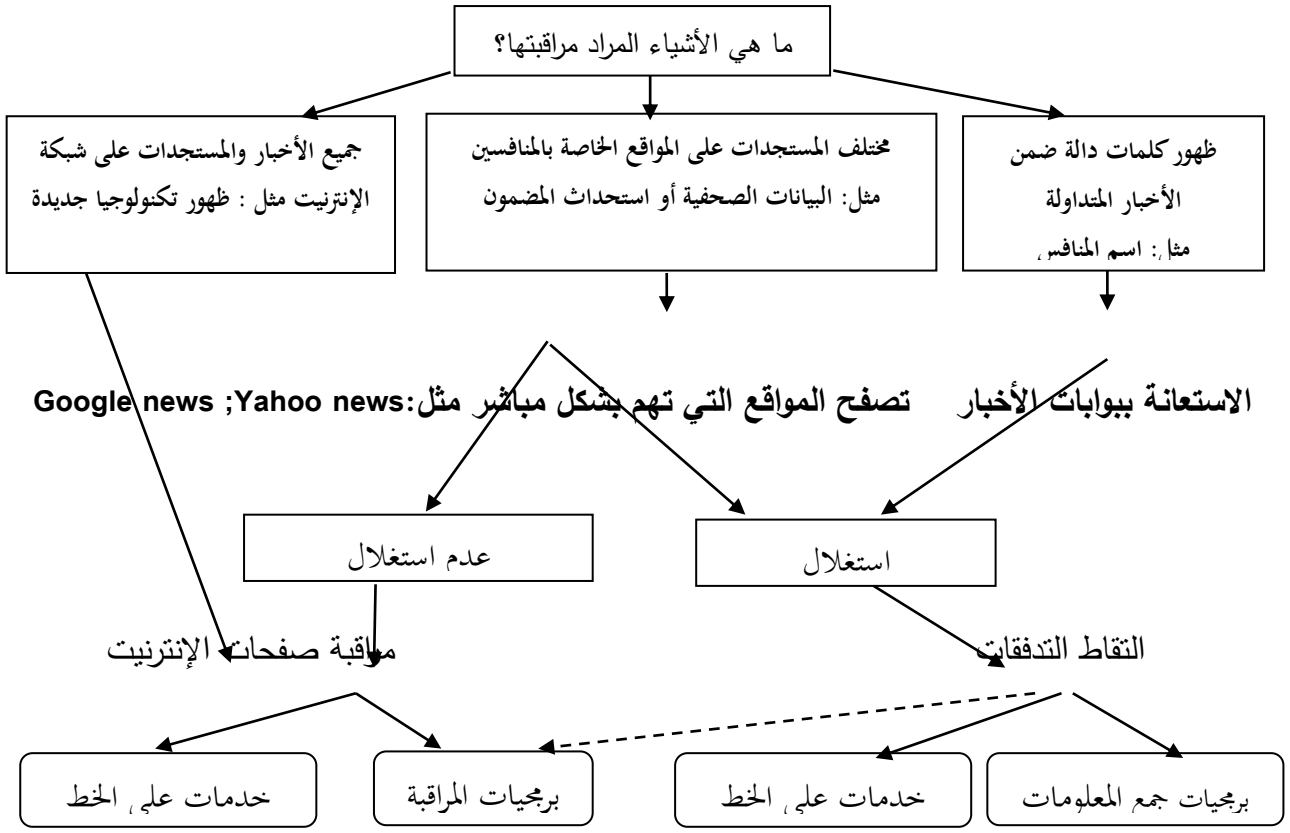
-اليقظة الهجومية أو مستوى التأثير: المستوى الثالث يتوافق مع ممارسات جد محددة لليقظة وفق أساليب هجومية تصل إلى حدود التجسس لكن دون تعديها،كأن يقوم أحد موظفي المؤسسة بتقديم نفسه كزبون يسعى للتعامل مع المنافس المباشر بهدف تقييم جودة الخدمات المقدمة من طرف تلك المؤسسات.وترتكز اليقظة الهجومية على مسار تقييمي مستمر لعناصر البيئة الخارجية بهدف تبني معارف جديدة وتطبيقها في المؤسسة،أو السعي نحو إقامة تحالفات مع مؤسسات أخرى بهدف التأثير في متغيرات البيئة وتعديلها لصالح المؤسسة، أي مساعدة المؤسسة على التحول من ردة الفعل إلى الفعل أي من التفاعل مع الأحداث والمتغيرات إلى استباق الأحداث. (Lendrevie, Levy, & Lindon, 2006, p. 203)

2.2.الإنترنيت المجال الحديث لليقظة.

تمنح الإنترنيت لمختلف المؤسسات إمكانية الوصول إلى مصادر جديدة للمعلومات ، ومقابل تكلفة محدودة، والأكيد أن استعمال هذه الوسيلة في اليقظة وجمع المعلومات ازداد بالنظر للتطور الكبير الذي شهدته هذه الوسيلة مع ظهور الجيل الثاني من الإنترنيت إلى غاية الجيل الرابع، والتي تعمل على وضع المستخدم في قلب هذا العالم الافتراضي،وما صاحب ذلك التطور من ظهور وسائل جديدة لمتابعة تدفق المعلومات مثل خدمة RSS* التي ساعدت على تبسيط استغلال المعلومات المنشورة على الإنترنيت وتصفية حجمها الكبير للاستفادة من تلك التي تعطي قيمة مضافة فقط(Deschamps, 2008, p. 52) .إلا أن ممارسة اليقظة على الإنترنيت واختيار الوسيلة المساعدة على ذلك يتوقف على الهدف المراد بلوغه وعلى طبيعة المعلومات المراد جمعها، ويمكن إيضاح أحد النماذج المقترحة لتطبيق اليقظة عبر الإنترنيت عبر الشكل الموالي:

الشكل رقم (01): اليقظة عبر الإنترنيت

*RSS Really Simple Syndication:.هي خدمة تمكن المستخدم من الاشتراك في المواقع بشكل مجاني والحصول عل آخر ما تم نشره ، فبدلا من تصفح المواقع والبحث عن المواضيع الجديدة، فإن هذه الخدمة تخطر المستخدم بما يستجد من معلومات فور نشرها.



المصدر: (Deschamps, , 2008, p. 53)

على كل يبقى النموذج الموضح مجرد اقتراح لتنظيم عمل اليقظة، فاستخدامات الإنترنيت غير محدودة وتتنوع استعمالاتها فإلى جانب المجالات المذكورة يمكن استغلال اليقظة للتعرف على ردة فعل الزبائن تجاه منتجات المؤسسة أو مدى تجاوبهم لعروضها الترويجية مثلا، وتبقى برمجيات المراقبة وجمع المعلومات أحد أهم الوسائل المساعدة على تسيير تطبيق اليقظة والرفع من كفاءة المعلومات التي يتم جمعها من خلالها.

واعتماد المؤسسة على الإنترنيت في ممارسة اليقظة، يساعدها بالدرجة الأولى على تبني "يقظة الصورة" والتي يتفرع عنها نوعين من اليقظة هما: "يقظة السمعة" و"يقظة الرأي"،أي رأي الزبائن حول المؤسسة والتي يتم قياسها بالأخص على شبكة الإنترنيت، ويبقى الهدف من يقظة الصورة هو مراقبة إدراك الزبائن والمستهلكين لصورة المؤسسة أو علامتها أو منتجاتها وكذلك صورة مسيريها وقادتها، كذلك تعمل في بعض الأحيان على الكشف المبكر للشائعات أو استباق أي أزمة إعلامية متعلقة بالمؤسسة. ويسعى هذا النوع لتقديم الإجابة عن الأسئلة التالية(Asselin, 2008, p. 67) :

-ما هي الآراء التي يتم تداولها حول المؤسسة، مورديها ومنتجاتها...الخ؟

- من هم الأطراف المسؤولين عن تشكيل المواقف تجاه المؤسسة، ومن يقوم بنشر الأخبار عنها؟

- ما هي سرعة انتشار المعلومات التي تخص المؤسسة على الإنترنيت أو على أرض الواقع؟

- ما هو أثر الأخبار المتداولة حول المؤسسة على صورتها وعلى مبيعاتها؟

3.2.إجراءات ممارسة اليقظة عبر الانترنيت.

تتمحور هذه الإجراءات حول عنصرين أساسين هما: وضع خطة البحث و توفير الوسائل لجمع المعلومات المطلوبة. و الأكيد أن خطة البحث الفعالة تبدأ دائما بتحديد ومعرفة مصادر المعلومات المختلفة. وتتنوع المصادر بحسب طبيعة المعلومات المراد الحصول عليها، ونظرا للحجم الكبير من المعلومات التي يمكن جمعا و نظرا لتشتت مصادرها كذلك، فإن تحقيق عملية يقظة شاملة يكاد يكون مستحيل. ولذلك فمن الضروري أن تنظم عملية اليقظة على الانترنيت بشكل ذكي خاصة وأنه في كثير من الأحيان ما يصعب رصد كل المصادر لنقص الوسائل البشرية والمادية أو لضعف الميزانية أو لضغط الوقت. ومع ذلك فإن المعلومات تخضع إلى بعض القوانين التي تساعد على هيكلة البحث بشكل فعال، ففي هذا الصدد وبحسب قانون "باريتو"* فإنه يمكن إيجاد 80% من المعلومات في 20% من المصادر الموجودة(Lopez da Silva, 2002, p. 36) .

ولكي تكون عملية جمع وتحصيل المعلومات متوافقة وصحيحة، يجب أن يؤخذ بعين الاعتبار كل مما يأتي (طالب، الشمرى، و الجنابى، 2003، الصفحات 72-73):

-الطلب المبكر: ذلك كون بعض المصادر تتطلب وقتا طويلا لاستغلالها

-الأسبقيات: تحديد الأسبقيات حسب متطلبات الوقت والمصدر وأولوية المعلومات المطلوبة.

-تعدد المداخل:أي اعتماد مصادر معلومات مختلفة للتخلص من الأخطاء التي قد ترد من أحد المصادر.

وعليه فإنه في هذه المرحلة يتم جمع المعلومات بشكل قانوني وأخلاقي من كافة المصادر المتاحة.

ما يجدر الإشارة إليه ، هو أن تحديد مصادر المعلومات وتصنيفها يتم وفقا لبعض المعايير، ولعل أهمها درجة الثقة التي يمكن أن تعطى لمحتوى كل مصدر ويتمثل العنصر الأكثر أهمية عند البحث عن تلك المصادر في تحديد أقلها تكلفة وأكثرها استيعابا للمعلومات (القهيوي، اللالا، و الوادي، 2013، صفحة 92).من جهة أخرى وقبل توجيه عملية اليقظة نحو المصادر الخارجية يجب التحقق من عدم توفر المعلومات المراد جمعها داخل المؤسسة، ففي كثير من الأحيان ما تكون المعلومات التي يحتاجها متخذ القرار متواجدة داخل المؤسسة إلا أنها تكون في شكل غير منظم.

وكمثال عن المعلومات التي يتم جمعها عن أحد المؤسسات المنافسة عن طريق اليقظة عبر الانترنيت، يمكن إبراز النقاط التسع الحرجة لتلك المؤسسات والتي يتم التركيز عليها، تتمثل تلك النقاط في: (Guichardaz, Lointier, & Rosé, 1999, p. 199)

-المعلومات الأساسية: تخص معلومات حول طبيعة نشاط المؤسسة وتنظيمها الداخلي.

-ثقافة المؤسسة: معلومات حول سلوك الموظفين والمسيرين.

-المعلومات المالية: تضم الوضعية الإقتصادية للمؤسسة وحجم نشاطها التجاري.

-الأهداف طويلة المدى: معرفة تموقع المؤسسة مقارنة بمنافسيها.

-معرفة مواقع تواجد المؤسسة: أي حدودها الجغرافية.

- دراسة منتجات المؤسسة: من خلال التعرف على العروض المقدمة لكل قسم من أقسام السوق.

-البحث والتطوير: وذلك عبر دراسة مؤشرات درجة الإبداع في المؤسسة.

* PARETO Vilfredo Frederico.

-الإستراتيجية التسويقية: بالتركيز أساسا على علاقتها بالسوق و بالموردين والزبائن.

-الموظفين: التعرف على تطور رأس المال البشري للمؤسسة.

4.2. أمن وحماية المعلومات في المؤسسة.

على الرغم من تعدد طرق حماية المعلومات وتطورها إلا أن هناك تطور مناظر لها بل وفي الغالب يتفوق عليها، وفي الغالب فإنه يترتب على اختراق أنظمة معلومات المؤسسة إما تدميره أو تعطيله أو الإستفادة المادية منه أو إفادة أشخاص على حساب أشخاص آخرين مما يترتب على خسائر للمؤسسات. إذ أن هناك بعض المعلومات الخاصة والسرية التي تعد ذات قيمة لإدارة المؤسسة يجب المحافظة عليها من المتطفلين ، وهي تمثل جزءاً من المخزون الملموس الذي يمثل تراكم الخبرة والمحاولات والأخطاء ، مثلاً البحث والتجارب خلال عدة سنوات ، هذه المعلومات كونها تتطلب إجراء وقائياً لحمايتها تصنف عادة بأنها خصوصية أو سرية ،ومن أمثلة المعلومات التي تتطلب الحماية يمكن ذكر مثلا: مواصفات تصميم المنتج ، تقارير النوعية ، أوراق البحث ، أسماء مجهزي المؤسسة وزبائنها ، خطط تطوير المنتجات ، الخطط المستقبلية للتوسع ، الإستراتيجيات التسويقية (درمان، فاعلية نظام المخابرات التسويقية في اتخاذ القرارات التسويقية،، 2003، صفحة 10). كل هذه المعلومات يمكن كشفها بصورة مباشرة أو غير مباشرة عن طريق استيلاء الأشخاص عليها ، هذه القيمة الضخمة للمعلومات يجب حمايتها والمحافظة عليها وهي تدخل تحت مفهوم أمن نظام اليقظة الاستراتيجية ، فالأكيد أن نظام اليقظة يهدف إلى مساعدة المؤسسة على استغلال الفرص لكن دون إغفال أهمية تحديد المخاطر والسعي نحو الحماية منها(Jakobiak, 2004, p. 335) ، فالأمن هو أحد أبعاد هذا النظام ومن أهم مراحله كذلك، هذا المفهوم يمكن إبرازه من ثلاث زوايا مختلفة هي (الألفي، 2007، صفحة 8):

-من زاوية تقنية : هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

-ومن زاوية قانونية : هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها .

-ومن زاوية أكاديمية : هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

وبصفة عامة فإن أمن نظام اليقظة يقتضي توفير الوسائل الخاصة التي تمنع أو تعيق حصول الأفراد غير المخولين على المعلومات السرية أو الخصوصية للمؤسسة.

5.2. عناصر المخاطر المهددة لليقظة عبر الانترنيت.

تنضوي تحت هذا البند مجموعة من العناصر التي تفيد في تحديد وتقدير المخاطر التي قد تتعرض لها المؤسسة عند ممارستها اليقظة عبر الانترنيت. ومن هذه العناصر:

- **الموارد:** تعتمد كثير من طرق تحليل المخاطر على تحديد وتصنيف موارد اليقظة التي تحتاج إلى برامج حماية والتي يعتقد أنها معرضة للانتهاك. ويمكن تصنيف الموارد حسب أهميتها أو قيمتها. ومن الموارد ذات العلاقة بنظام اليقظة ما يلي(Löning, Malleret, Méric, Pesqueux, & Sole, 2008, p. 212) :

-البيانات والمعلومات.

-المكونات المادية والبرمجية.

-الوثائق.

-الأفراد.

- **مصادر الخطر:** وهناك عدد كبير من الأخطار التي تؤثر على نظم اليقظة عبر الانترنيت ومنها (العجيلي، 2004، صفحة 04):

-الأخطاء.

-التخريب المتعمد.

-الاحتيال والتزوير.

-السرقات.

-الخلل في المعدات والبرمجيات.

-الإختراق:وفي أغلب الأحيان يتم الاختراق بطريقتين (الغمري، 2012، الصفحات 126-127):

*المخترق الداخلي:يتم عن طريق الأفراد الذين يعملون في المؤسسة،وهؤلاء أشد قدرة على اختراق سرية المعلومة ، وغالبا ما تقوم المؤسسة بحل المشكلة بكل سرية حتى لا يؤثر ذلك على سمعتها وفقدان الثقة من قبل زبائنها، وقد يقوم المخترق الداخلي بتوفير نقاط العبور والممرات الالكترونية للغير للاطلاع على أسرار المؤسسة لما لديه من تسهيلات أكثر من المخترق الخارجي إضافة إلى درايته بأنظمة المؤسسة وخباياها وإمكانية وصوله للمعلومات الحساسة.

*المخترق الخارجي:ويتم ذلك إما بانتحال الشخصية أو محاولة استقطاب شخص من داخل المؤسسة ،كما يتم الاعتماد على الفيروسات ، والفيروسات هي أي برامج أو مجموعة من التعليمات التي تلحق الضرر بنظام اليقظة على أن تكون لديها القدرة على و التضاعف والانتشار (حسن، 2004، صفحة 102).

- **نقاط الضعف:** إن تحليل مصادر الخطر تفيد في تحديد مجموعة نقاط ضعف ومنها (شكر، 2010، صفحة 224):

-ضعف في التدريب.

-ضعف في إجراءات الحماية والأمان.

-اختيار كلمات سر غير مجربة.

-اعتماد تقنية غير مجربة.

-البث عبر خطوط غير محمية.

6.2. مظاهر أمن وحماية المعلومات في المؤسسة

يمكن تحديد مظاهر أو أوجه حماية نظام اليقظة بآلاتي (درمان، فاعلية نظام المخابرات التسويقية في اتخاذ القرارات التسويقية،، 2003، صفحة 10) :

-**الأمن المادي** :ويتعلق باتخاذ الاحتياطيات الملائمة لحماية المؤسسة والمعلومات من الغرباء والباحثين عن السرقة والاستيلاء والتطفل لغرض الحصول على المعلومات وإلحاق الأذى والضرر بالمنظمة ووسائل الأمن المادي وتتضمن: كلمات السر، الأجهزة الالكترونية المستخدمة في عكلية اليقظة عبر الانترنيت .

- **أمن الأفراد**:وهو يتعلق بالمستخدمين الذين يتصلون مع الغرباء مثل الموظفين المحتملين ، المجهزين ، المستهلكين، وكذلك ما يتعلق بمخاطر الأمن في تشغيل مستخدمين جدد، لذلك ينبغي التركيز على معلومات عن الأفراد وسلوكياتهم وطباعهم وسماتهم الشخصية وغيرها من المعلومات .

- **أمن الاتصالات** :وهو ما يتعلق باتخاذ الاحتياطيات الخاصة بالمعلومات المنقولة أو المكتوبة بأساليب الكترونية ويتم حماية الاتصالات عن طريق تشفير المعلومات .

-**أمن التكنولوجيا**: تهدف إلى حماية نظام اليقظة من الأفراد والمجموعات التي تستخدم الحيل كالربط الهاتفي وأجهزة التنصت .

7.2. العناصر الأساسية لحماية نظام اليقظة في المؤسسة.

ليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء ،وليس كل المعلومات في المؤسسة الواحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها ، لذا يجب أن نحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية ، إذ تصنف المعلومات تبعا لكل حالة على حده ، من معلومات لا تتطلب الحماية ، إلى معلومات تتطلب حماية قصوى (الألفي، 2007، صفحة 10)،فالدراسات أثبتت أن المعلومات التي تستدعي الحماية هي المعلومات الرمادية والسوداء والتي لا تتجاوز نسبتها 10% من إجمالي المعلومات التي تمتلكها المؤسسة (Alexandre-Leclair, 2001, p. 123).

فيجب توضيح بعض النقاط التي تدخل ضمن أبجديات عمل نظام اليقظة والتي تضمن له جزء من الحماية اللازمة وبصفة آلية والتي تدخل ضمن متطلبات إنشاء هذا النظام، وتتمثل هذه العناصر في:

-السرية: أي التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص) (صقر، 2007، الصفحات 04-05).

- التحقق من الهوية: إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

-الكمال : تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

- التوفر:الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.

– مكافحة الإنكار (المسؤولية):التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات (مكاوي، 2009، صفحة 01).

7.2 طرق ووسائل حماية نظام اليقظة.

لضمان أفضل حماية لنظام اليقظة عبر الانترنيت لا بد من براز أهم تقنيات الحماية الواجب اعتمادها كما يلي:

–**توعية الموظفين والعمال بطرق حماية وأمن المعلومات:** على المؤسسة أن تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن قبل التفكير في تطبيق أي وسيلة لحماية النظام ، بل المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الإجراءات المتطلبة من الكل لدى ملاحظة أي خلل ،لذلك يجب إقناع العاملين بأن ضمان حماية معلومات المؤسسة هو ضمان لمنصب عمله وأن احترام قواعد الأمن سيجنبهم العقاب(Bisson, 2003, p. 75) .

–**التوثيق** : بشكل رئيس فان التوثيق لازم وضروري لنظام التعريف والتخويل، وتصنيف المعلومات. وفي إطار الأمن ، فان التوثيق يتطلب أن تكون إستراتيجية أو سياسة الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق ، إضافة إلى خطط التعامل مع المخاطر والحوادث ، والجهات المسؤولة ومسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بنظام اليقظة عند حدوث الخطر (الألفي، 2007، صفحة 13).

–**تصنيف المعلومات** : وهي عملية أساسية لدى ممارسة اليقظة عبر الانترنيت، وتختلف التصنيفات حسب احتياجات المؤسسة، فمثلا قد تصنف المعلومات إلى معلومات متاحة ، وموثوقة ، وسرية ، وسرية للغاية أو قد تكون معلومات متاح الوصول إليها وأخرى محظور التوصل إليها وهكذا (صقر، 2007، صفحة 10).

–**التحقق من هوية المستخدمين:**طالما أن الشخص الذي يستطيع أن يتعامل مع نظام اليقظة من الممكن أن يقوم بتغيير أو نسخ أو مسح بعض أو كل البيانات أو المعلومات – سواء عمداً أو بدون عمد – فإن هذا يمثل خطراً كبيرا، لذلك فإنه يجب وضع العديد من الحواجز المادية والأرقام السرية وبعض أساليب التعرف علي الشخص بالإضافة إلي بعض أساليب الوقاية الإجرائية لكل مستخدم. فعلى سبيل المثال يكون هناك رقم مرور سري للدخول في النظام، ثم رقم آخر للدخول في جزء معين لقواعد البيانات، ورقم ثالث للدخول إلي البرامج. أيضاً يتم إعطاء كل شخص رقم سري للدخول والتعامل مع البيانات التي تخصه فقط وحسب مسؤولياته، فالبعض يكون له الحق في الإطلاع علي البيانات أو النتائج فقط، والبعض له حق التغيير وآخرين لهم حق تغيير الإجراءات التي يتم معالجة البيانات بها.

–**التشفير:** تحظى تقنيات التشفير باهتمام في ميدان أمن المعلومات، ومرد ذلك أن حماية بالتشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة ، السرية والتكاملية وتوفير المعلومات ، فضمان سرية المعلومات أصبح يعتمد من بين ما يعتمد على تشفير وترميز الملفات والمعطيات بل تشفير وسائل التثبت وكلمات السر ، كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتثبت لدى فك التشفير أن محتوى

المعلومات لم يتعرض لأي نوع من التعديل أو التغيير، ويعد التشفير بوجه عام وتطبيقاته العديدة ، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية (AFFRES, et al., 2003, p. 83) . وبذلك فان التشفير يمثل الإستراتيجية الشمولية لتحقيق أهداف الأمن من جهة ، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى ، خاصة في بيئة الأعمال الالكترونية وعموما البيانات المتبادلة بالوسائط الإلكترونية .

– **استخدام برمجيات الحماية:** لا يمكن اعتبار أية سياسة أمنية شاملة، ما لم يتم الاعتناء بأمن البرمجيات المستخدمة، فيجب على المؤسسة أن تختبر الأنظمة الدفاعية التي تحمى نظام اليقظة بصفة دورية و مستمرة و ذلك عن طريق مهاجمته باستخدام برامج خبيثة أو فيروسات لاختبار برامج الحماية، كما يتم استخدام الجدران النارية Firewalls لحماية النظام من اختراق المهاجمين من خارج المؤسسة، إضافة إلى استخدام برامج الحماية من الفيروسات الإليكترونية لأن برامج Firewalls نادرا ما تقدم وسائل الحماية من هذه الفيروسات و إذا قدمت وسيلة للحماية فإنها في الأغلب تكون وسيلة ضعيفة ومحدودة في حماية النظام (الدايم، 2004، صفحة 22).

3. الدراسة التطبيقية:

1.3. الطريقة والأدوات:

من أجل الوصول إلى إجابة علمية على التساؤل الرئيسي ، قمنا باختيار عينة محددة من مجتمع الدراسة ولهذا الغرض ولأجل القيام بجمع البيانات من عينة الدراسة تم الاعتماد بشكل أساسي على قائمة استقصاء، والتي قمنا بتصميمها لجمع البيانات الأولية اللازمة لاختبار فرضيات الدراسة. وقد تضمنت القائمة المقاييس الخاصة بمتغيرات الدراسة.

بسبب عدم توفرنا على قاعدة بيانات تحمل كل المعلومات الخاصة بكل أفراد مجتمع الدراسة، اضطررنا إلى استعمال الطريقة غير العشوائية في المعاينة بدلا من الطريقة العشوائية،وبسبب التخوف من مشاكل في جمع الأجوبة و التقدير ارتأينا أن يكون مجتمع هذه الدراسة هو المؤسسات الاقتصادية التي تنشط في منطقة الوسط. فيما يخص نوع العينة فقد اعتمدنا على العينة التيسيرية، وهي عبارة عن المؤسسات التي رأينا أنه من السهل علينا الحصول على موافقة المسؤولين فيها للإجابة على قائمة الاستقصاء ،أما بالنسبة لحجم العينة فقد قمنا بتحديده في 30 مؤسسة وهو عدد المؤسسات التي تجاوبت مع دراستنا.

قدر معامل الثبات لفقرات الاستقصاء المستخدمة في اختبار فرضيات الدراسة ب 0.896 وهو ما يدل على أن الدراسة تتميز بثبات حيد، كما أن معامل الصدق قدر ب 0.946، ويدل هذا بصفة عامة على وجود درجة عالية من الثبات والصدق لإجابات المستقصى منهم على العبارات الواردة بقائمة الاستقصاء.

2.3. تحليل الوصفي لقوائم الاستقاء:

سوف نستعرض من خلال هذا الجزء لنتائج التحليل الوصفي لعينة الدراسة ، من خلال حساب كل من المتوسط الحسابي المرجح والانحراف المعياري لأقسام الاستبيان التي تحتوي أسئلة السلم ، إضافة إلى عرض التكرارات ونسب الإجابات حول السؤال المغلق.

1.2.3. تحليل الأجوبة الخاصة بمدى تنظيم عملية جمع المعلومات عبر الإنترنيت في المؤسسات محل الدراسة:

للتأكد من التبني الفعلي لنظام اليقظة عبر الانترنيت بغض النظر عن ما إذا كان في شكل منظم أم في شكل ممارسات تقوم بها المؤسسات ضمن أنشطتها اليومية، قمنا بطرح هذا سؤال مغلق للتأكد من مدى تطبيق مفردات الدراسة لسياسة محدد المعالم للبحث عن المعلومات عبر الانترنيت واستغلالها، وقد كانت الإجابة وفق ما يوضحه الجدول التالي:

جدول رقم (01): الأجوبة الخاصة بامتلاك سياسة لجمع المعلومات عبر الانترنيت

العبارة	نعم		لا	
	التكرار	النسبة	التكرار	النسبة
تمتلكون في مؤسستكم سياسة محددة ومنظمة لجمع المعلومات على الانترنيت	10	% 33,33	20	% 66,67

المصدر : من إعداد الباحثين بناء على تحليل نتائج الاستقصاء.

من خلال النتائج الموضحة في الجدول أعلاه يتضح أن66,67 % من عينة الدراسة أقرت بتواجد سياسة محددة ومنظمة للبحث عن المعلومات على الانترنيت،مما يدل على تبنيها لليقظة لجمع المعلومات المرتبطة بنشاطها على من خلال المصادر التي تتيحها الإنترنيت،بينما النسبة الباقية والمقدرة ب 33,33% لا تمتلك سياسة واضحة المعالم للبحث على الانترنيت، لكن هذا لا يعني أنها لا تستخدم الانترنيت للبحث عن المعلومات، أو أنها لا تمارس اليقظة، وللتحقق من ذلك قمنا بصياغة الجزء الموالي من قائمة الاستبيان، للتعرف إذا ما كانت هذه المؤسسة تمارس اليقظة دون تبنيها لسياسة واضحة لذلك.

2.2.3. تحليل الأجوبة الخاصة بممارسة اليقظة عبر الإنترنيت في المؤسسات محل الدراسة:

حاولنا من خلال هذا الجزء معرفة مدى استغلال مؤسسات العينة للإنترنيت في جمع المعلومات بواسطة اليقظة حيث جاءت النتائج كما يوضحها الجدول رقم **2**.

جدول رقم (02): الإحصاءات الوصفية لاستغلال شبكة الإنترنيت في ممارسة اليقظة

العبـارة	المتوسط الحسابي المرجح	الانحراف المعياري	الاتجاه	الترتيب
1-تستخدمون وسائل آلية لجمع المعلومات عبر الإنترنيت	3,77	,847	غالبا	1
2-تتحققون دوريا من تواجد مؤسستكم في الصفحات الأولى لمحركات البحث	3,90	,960	غالبا	5
3-تبحثون عن المواضيع المرتبطة بمؤسستكم والتي يتابعها رواد الإنترنيت	3,13	1,008	أحيانا	12
4-تتواجد مؤسستكم في مواقع التواصل الاجتماعي	3,80	,858	غالبا	6
5-هناك روابط بين موقعكم الالكتروني و مواقع التواصل	3,03	,809	أحيانا	13

الاجتماعي				
6-تقومون بتقييم صورة علامتكم دوريا على شبكة الإنترنيت	**3,43**	**,728**	**غالبا**	**8**
7- تقومون بقياس شهرة مؤسستكم عبر شبكة الانترنيت.	**4,10**	**,803**	**غالبا**	**1**
8-تتابعون تواجد زبائنكم في موقع مؤسستكم الالكتروني	**3,03**	**1,066**	**أحيانا**	**14**
9- تتابعون ظهور و تواجد منافسيكم عبر شبكة الإنترنيت	**4,10**	**,885**	**غالبا**	**2**
10- تتابعون ظهور و تواجد مورديكم عبر شبكة الإنترنيت	**3,33**	**,758**	**أحيانا**	**9**
11- تتابعون عبر شبكة الإنترنيت ظهور و تواجد موزعي منتجاتكم	**3,00**	**,788**	**أحيانا**	**16**
12- تدرسون كيف يتلقى رواد الإنترنيت خطابكم التسويقي	**2,87**	**,860**	**أحيانا**	**17**
13-تتحكمون في المضمون وفي الصورة التي يتم تداولها حول مؤسستكم عبر الإنترنيت	**3,33**	**1,155**	**أحيانا**	**10**
14-تراقبون التعليقات المتداولة حول مؤسستكم عبر الإنترنيت	**3,97**	**,809**	**غالبا**	**4**
15-تحرصون على عدم تحريف صورة مؤسستكم وتعليقاتكم عبر الإنترنيت	**4,03**	**,890**	**غالبا**	**3**
16-تمتلكون في مؤسستكم سياسة لتكوين السمعة عبر الإنترنيت é-réputation	**3,27**	**1,258**	**أحيانا**	**11**
17- تأخذون بعين الاعتبار سياسة السمعة عبر الانترنيت ضمن إستراتيجيتكم التسويقية	**3,03**	**1,402**	**أحيانا**	**15**
المعدل العام	**3,4784**	**,65243**	**غالبا**	

المصدر : من إعداد الباحثين بناء على تحليل نتائج الاستقصاء.

بالتفصيل في النتائج المتحصل عليها نجد أن كل العبارات جاء اتجاهها بين "أحيانا و"غالبا"، حيث نلاحظ أن أغلب المؤسسات تقوم بقياس الشهرة عبر شبكة الانترنيت، و كذلك متابعة ظهور و تواجد منافسيها عبر شبكة وهما النشاطين الذين حازا أكبر متوسط حسابي والمقدر ب 4,10 ، وقد جاء في المرتبة الثالثة عمل المؤسسة على عدم تحريف صورتها وتعليقاتها عبر الإنترنيت بتوجه "غالبا"، وما يؤكد ذلك إقرار المؤسسات بمراقبة التعليقات المتداولة حولها عبر الإنترنيت والذي جاء في المرتبة الرابعة بمتوسط حسابي 3,97 .فضلا عن المتابعة المستمرة لتواجد المؤسسات في الصفحات الأولى لمحركات البحث والذين حاز على متوسط حسابي قيمته 4,90 . وكذلك إقرار المؤسسات بتواجدها في مواقع التواصل الاجتماعي بامتلاكها لصفحات على مختلف المنصات والذي جاء عند توجه "غالبا".

الملاحظ كذلك هو توجه أغلب المؤسسات إلى استخدام وسائل آلية لجمع المعلومات عبر الإنترنيت بمتوسط حسابي قيمته 3,77 ، وهو الأمر الذي يسهل عمليه الحصول على المعلومات ذات الصلة بنشاط المؤسسة بصفة آلية وبطريقة سريعة دون الحاجة على جهد بشري.ومن الأنشطة التي تمارسها المؤسسات محل الدراسة

بصفة كبيرة أيضا هي تقييم صورة علامتها دوريا على شبكة الإنترنيت والتي جاءت بتوجه "غالبا" بمتوسط حسابي قيمته 3,43.

أما باقي الممارسات المرتبطة باليقظة على الانترنيت فقد جاءت إجابة المؤسسات عنها كلها عند مستوى "حاليا"، مع اختلاف في متوسطاتها الحسابية، أين نجد قيامها بمتابعة ظهور و تواجد مورديها عبر شبكة الإنترنيت، والتحكم في المضمون وفي الصورة التي يتم تداولها حول المؤسسة عبر الإنترنيت بمتوسط حسابي 3,33 ، بنما قدر المتويط الحسابي للمؤسسات التي تمتلك مؤسستكم سياسة لتكوين السمعة عبر الإنترنيت ب 3,27، ثم 3.13 كمتوسط حسابي لنشاط البحث عن المواضيع يتابعها رواد الإنترنيت والتي تخص المؤسسات محل الدراسة 3,13، في حين جاءت كل من وضع روابط بين الموقع الالكتروني للمؤسسة ومواقع التواصل الاجتماعي، وكذلك متابعة تواجد الزبائن في الموقع الالكتروني للمؤسسة،و الأخذ بعين الاعتبار سياسة السمعة عبر الانترنيت ضمن الإستراتيجية التسويقية بمتوسط حسابي 3,03 لكل منها.لتليها متابعة ظهور و تواجد موزعي منتجاتها عبر شبكة الإنترنيت بمتوسط قيمته 3,00، أما المرتبة الأخيرة فتمثلت في دراسة المؤسسات لكيفية تلقي رواد الإنترنيت لخطابهم التسويقي والذي جاء بمتوسط حسابي 2,87، رغم أهمية هذا النشط الذي يدخل ضمن اليقظة التسويقية لما له من أهمية في معالجة النقائص التي قد تقع فيها المؤسسات عند صياغة إستراتيجيتهم التسويقية.

وجدنا في القسم السابق أن 66,67% من عينة الدراسة أقرت بتواجد سياسة محددة ومنظمة للبحث عن المعلومات على الانترنيت ، لكن الواضح من خلال الجدول (2) أن أغلب المؤسسات تمارس في الواقع العملي نشاط يدخل في إطار اليقظة عبر الانترنيت، كون أن معدل المتوسط الحسابي لإجمالي العبارات قدر ب**3,4784**، وهذا إن دل على شيء فإنما يدل على أن عدم تواجد بتواجد سياسة محددة ومنظمة للبحث عن المعلومات على الانترنيت وفق الشكل الذي جاء في الجزء النظري ليس مؤشرا على عدم استغلال الانترنيت لممارسة نشاط اليقظة كما هو الحال بالنسبة لمؤسسات العينة.

3.2.3. تحليل الأجوبة الخاصة بأمن وحماية المعلومات في المؤسسات محل الدراسة:

تظهر النتائج المرتبطة بهذا الجزء اهتماما كبير من قبل المؤسسات بحماية وأمن المعلومات بجوانبه المختلفة سواء الأمن المادي أو أمن الأفراد و كذا أمن الاتصالات والتكنولوجيا، فالاتجاه العام لتطبيق عناصر الأمن والحماية جاء عند مستوى "غالبا"

الجدول رقم (03): الإحصاءات الوصفية لأمن وحماية المعلومات ضمن عينة الدراسة

العبارة	المتوسط الحسابي المرجح	الانحراف المعياري	الاتجاه	الترتيب
1-أجهزة السيرفر وأجهزة الكمبيوتر في مؤسستكم مزودين ببرمجيات الحماية ضد الفيروسات وضد الاختراقات الالكترونية، وبالجدران النارية.	**4,37**	**,490**	**دائما**	**5**
2- في مؤسستكم المعلومات الحساسة تخضع لوسائل حماية خاصة.	**4,40**	**,563**	**دائما**	**4**

3–تقومون بتشفير المعلومات الحساسة	**3,70**	**,952**	**غالبا**	**6**
4–تقومون بتدريب موظفيكم على تقنيات التشفير.	**2,80**	**,997**	**أحيانا**	**7**
5– تقومون باستعمال كلمة سر شخصية لحماية كل أجهزة الكمبيوتر	**4,60**	**,498**	**دائما**	**3**
6–تجتنبون استعمال شبكات التواصل الاجتماعي للحديث عن مؤسستكم، ما عدى في إطار نشاط تسويقي مخطط	**4,70**	**,466**	**دائما**	**2**
7– تلتزمون بواجب السرية تجاه نشاطكم المهني عند استخدامكم للأنترنيت	**4,73**	**,450**	**دائما**	**1**
المعدل العام	**3,9417**	**,60148**	**غالبا**	

المصدر : من إعداد الباحثين بناء على تحليل نتائج الاستقصاء.

تظهر النتائج الموضحة في الجدول الالتزام التام بقواعد أمن وحماية المعلومات ضمن عينة الدراسة، فالملاحظ أن المستقصى منهم بواجب يلتزمون السرية تجاه نشاطكم المهني وذلك بعدم الحديث عن أسرار عملهم خارج المؤسسة والتي جاءت في المرتبة الأولى من حيث الإجابات وبمتوسط حسابي قدره 4,73، نفس الشيء فيما يخص التزامهم بعدم استعمال شبكات التواصل الاجتماعي للحديث عن المؤسسة ، والذي لا يتم إلا في إطار نشاط تسويقي مخطط حيث أن المتوسط الحسابي لهذا العنصر قيمته 4,70. الملاحظ كذلك الأهمية التي توليها المؤسسات للأمن المادي حيث أن المؤسسات تقوم باستعمال كلمة سر شخصية لحماية كل أجهزة الكمبيوتر باتجاه "غالبا"إلى "دائما" وبمتوسط حسابي قدره 4,60 تقوم المؤسسات كذلك باتخاذ إجراءات حماية خاصة بالمعلومات الحساسة مثل الإستراتيجية العامة والمنتجات والخدمات التي تنوي تطويرها، حيث جاء هذا العنصر في المرتبة الرابعة بمتوسط حسابي قيمته 4,40،إضافة إلى تزويد أجهزة السيرفر وأجهزة الكمبيوتر في المؤسسات ببرمجيات الحماية ضد الفيروسات وضد الاختراقات الالكترونية، وبالجدران النارية، أين كانت كل الإجابات باتجاه "دائما" وقدر المتوسط الحسابي لهذا العنصر ب4,37 ، كما تخضع هذه المعلومات للتشفير من طرف المؤسسات باتجاه "غالب. لكن الملاحظ في الأخير أن هناك انخفاض لدى المؤسسات في توجهها نحو تدريب الموظفين على تقنيات التشفير عند مستوى "أحينا" وذلك بمتوسط حسابي قدره 2,80.

4.3. اختبار الفرضيات:

يهدف هذا الجزء إلى عرض ومناقشة نتائج اختبار فرضيات الدراسة بتفرعاتها، وذلك في إطار الأهداف التي سعت هذه الدراسة إلى تحقيقها على النحو التالي:

1.4.3. اختبار الفرضية الأولى: "لا توجد فروق ذات دلالة إحصائية في تطبيق اليقظة على الانترنيت في المؤسسات محل الدراسة تعود لامتلاكها سياسة محددة ومنظمة لجمع المعلومات على الانترنيت"

حيث يظهر الجدول الموالي نتائج اختبار الفرضية.

الجدول رقم (04): تحليل التباين الأحادي (ANOVA) لاختبار الفروق في تطبيق اليقظة على الانترنيت حسب امتلاك المؤسسات لسياسة محددة ومنظمة لجمع المعلومات على الانترنيت

المتغير المستقل	مصدر التباين	مجموع المربعات	متوسط المربعات	قيمة (F)	مستوى الدلالة
حجم النشاط	بين المجموعات	3,318	1,106	3,186	*0,04
	داخل المجموعات	9,026	,347		

* ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$).

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي.

يتضح من خلال الجدول أعلاه أن قيمة (F) المحسوبة (3,186) دالة إحصائياً عند مستوى معنوية أقل من (0,05) وعليه ترفض فرضية العدم وتقبل الفرض البديل ، وهو وجود فروق ذات دلالة إحصائية عند مستوى $\alpha \geq 0.05$ في تطبيق اليقظة على الانترنيت باختلاف تواجد سياسة محددة ومنظمة لجمع المعلومات على الانترنيت في المؤسسات محل الدراسة .

2.4.3. اختبار الفرضية الثانية: "لا توجد فروق ذات دلالة إحصائية في مستوى أمن وحماية المعلومات في المؤسسات محل الدراسة تعود لامتلاكها سياسة محددة ومنظمة لجمع المعلومات على الانترنيت "

حيث يظهر الجدول الموالي نتائج اختبار الفرضية.

الجدول رقم (05): تحليل التباين الأحادي (ANOVA) لاختبار الفروق في مستوى أمن وحماية المعلومات حسب امتلاك المؤسسات لسياسة محددة ومنظمة لجمع المعلومات على الانترنيت

المتغير المستقل	مصدر التباين	مجموع المربعات	متوسط المربعات	قيمة (F)	مستوى الدلالة
حجم النشاط	بين المجموعات	,546	,182	,476	0,702
	داخل المجموعات	9,946	,383		

* غير دالة إحصائيا عند مستوى ($\alpha \leq 0.05$).

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي.

يتضح من خلال الجدول أعلاه أن قيمة (F) المحسوبة (0,476) غير دالة إحصائياً عند مستوى معنوية أقل من (0,05) وعليه تقبل فرضية العدم ، وهي عدم وجود فروق ذات دلالة إحصائية عند مستوى $\alpha \geq 0.05$ في مستوى أمن وحماية المعلومات باختلاف تواجد سياسة محددة ومنظمة لجمع المعلومات على الانترنيت في المؤسسات محل الدراسة .

3.4.3. اختبار الفرضية الثالثة: "لا يوجد أثر ذو دلالة إحصائية بين اليقظة على الانترنيت ومستوى أمن وحماية المعلومات في المؤسسات محل الدراسة "

حيث يظهر الجدول الموالي نتائج اختبار الفرضية.

الجدول رقم (06):نتائج تحليل التباين للانحدار (ANOVA) للتأكد من صلاحية النموذج لاختبار الفرضية

المتغير المستقل	المصدر	مجموع المربعات	متوسط المربعات	قيمة (F)	مستوى الدلالة	معامل التحديد R^2	معامل الارتباط R
اليقظة على الانترنيت	الانحدار	1,366	1,366	3,485	*0,032	0,452	0,667
	الخطأ	10,978	,392				
	المجموع	12,344					

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي.

يتبين من معطيات الجدول رقم (6) أن قيمة (F) المحسوبة (اليقظة على الانترنيت) دالة إحصائياً عند مستوى معنوية أقل من (0,05). ويتضح من نفس الجدول أن المتغير المستقل (اليقظة على الانترنيت) في هذا النموذج يفسر ما مقداره (45.2%) من التباين في المتغير التابع (أمن وحماية المعلومات)، وهي قوة تفسيرية جيدة نسبياً، أما النسبة الباقية البالغة (54.8%) فتعود لمساهمة متغيرات أخرى غير داخلة ضمن نموذج الدراسة. كما يوضح معامل الارتباط (0,667) وجود ارتباط موجب قوي بين اليقظة على الإنترنيت و مستوى أمن وحماية المعلومات في المؤسسة.

بناءا على ما سبق يمكن اعتبار أن هناك أثراً مهماً للمتغير المستقل (اليقظة على الانترنيت) في المتغير التابع (أمن وحماية المعلومات)، وبذلك تثبت صلاحية النموذج لاختبار الفرضية.

وقد تم استخدام تحليل الانحدار البسيط لاختبار هذه الفرضية، حيث يوضح الجدول التالي تقدير معلمات هذا النموذج من أجل قياس أثر اليقظة على الانترنيت على أمن وحماية المعلومات.

الجدول رقم (7):نتائج تحليل الانحدار البسيط لبيان أثر اليقظة على الانترنيت و أمن وحماية المعلومات.

النموذج	معاملات غير معيارية		معامل معياري Beta	قيمة (T) المحسوبة	مستوى دلالة (T)
	B	الخطأ المعياري			
الثابت	2,536	,518		4,897	*0,000
اليقظة على الانترنيت (x)	,457	,338	676,0	,8673	*0,032

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي.

يتضح من الجدول أعلاه أن قيمة المعامل المعياري 0,667 أي أن قوة العلاقة بين اليقظة على الانترنيت والإقبال على طلب الخدمات الالكترونية 66,7 % .

بالنسبة لاختبارات معنوية معاملات الانحدار يتضح من الجدول السابق أن قيمة (T) المحسوبة (3,867) للمتغير المستقل ذات دلالة إحصائية عند مستوى معنوية أقل من (0,05).

بناءا على ما تقدم فإننا نقبل الفرضية بصيغتها.

4. الخاتمة:

من خلال دراستنا توصلنا إلى أن التحدي الكبير للمؤسسات اليوم يتمثل في القيام باليقظة بطريقة فعالة، من خلال بناء نظام قوي يسمح برصد كل ما يحدث في البيئة واستشراف اتجاهاتها المستقبلية.ففي ظل بيئة شديدة الديناميكية وبتزايد حدة المنافسة فيها أصبحت المؤسسات مجبرة على استغلال كل الوسائل والأدوات المتاحة للمحافظة تنافسيتها، وتعتبر اليقظة عبر الإنترنيت أحد أهم تلك الوسائل لما توفره من مصادر للمعلومات الفعالة.

من جهة أخرى فإن أمن المعلومات هو من أمن المؤسسة، هذا الأخير يعتمد في الأساس على الإدارة وليس على الأساليب التكنولوجية فقط فلابد من إدارة ممتازة وإجراءات تشغيلية وتنفيذ دقيق لكي يكون تركيب الوسائل التكنولوجيا مثل برامج الحماية ناجحا ومؤثراً، كما ولابد للمؤسسة أن تمتلك نظاماً للأمن الشامل وهذا يعنى أن تقفل كل الطرق والوسائل التي قد يأتي منها الهجوم عند استعمالها للإنترنيت في عملية اليقظة.

ومن أهم النتائج التي توصلنا إليها من خلال الدراسة التطبيقية ، نذكر:

– أن أغلب المؤسسات تمارس في الواقع العملي نشاط يدخل في إطار اليقظة عبر الانترنيت،حتى تلك التي ليس لديها سياسة ومنهجية واضحة لغدارة هذا النشاط

– وجود فروق في تطبيق اليقظة على الانترنيت في المؤسسات محل الدراسة حسب امتلاكها ل سياسة محددة ومنظمة لجمع المعلومات على الانترنيت.

– يوجد أثر واضح لممارسة اليقظة على الانترنيت على مستوى أمن وحماية المعلومات في المؤسسات محل الدراسة، أي أن المؤسسات التي تمارس هذا النشاط بشكل ممنهج لديها أنظمة امن وحماية اكبر.

من أهم الاقتراحات التي يمكن تقديمها ندكر:

– لابد على المؤسسات أن تحدد الأولويات عند القيام بنشاط اليقظة عبر الإنترنيت،إذ أنه من الصعب وحتى من المستحيل معرفة و مراقبة واستغلال كل المصادر التي توفرها الإنترنيت والتي لها علاقة بالمتغيرات التي تتحكم في نشاط المؤسسة.فالغاية من الاستهداف هي التعرف على مراكز الاهتمام وحصر النطاق البيئي الذي يجب وضعه تحت المراقبة.

– يجب اتخاذ تدابير وقائية حتى تتجنب المؤسسة التعرض لمخاطر الاختراق أو سرقة المعلومات عند القيام باليقظة عبر الإنترنيت،ك استخدام أنظمة قوية لتشفير المعلومات المرسلة، و تركيب أنظمة كشف الاختراق وتحديثها، فضلا عن تركيب أنظمة مراقبة شبكة الانترنيت للتنبيه إلى نقاط الضعف والثغرات الأمنية، مع نشر الوعي الأمني المعلوماتي بين موظفي المؤسسة،وتوعيتهم بأهمية الالتزام بقواعد أمن وسرية المعلومات.

–ضرورة تكوين الموظفين في مختلف المستويات الإدارية على طرق وأساليب اليقظة عبر الإنترنيت ومراقبة مصادر المعلومات المختلفة ذات الصلة بنشاطهم، وكيفية تحليلها.

5.المراجع:

1.5. المراجع باللغة العربية:

1.1.5. الكتب:

– داود طاهر حسن. (2004). *أمن شبكات المعلومات*. السعودية: مركز البحوث، معهد الإدارة العامة.

– علاء فرحان طالب، محمد جبار الشمرى، و حسين الجنابى. (2003). نظام الإستخبارات التسويقية. الأردن: دار الصفاء للنشر والتوزيع.

– ليث عبد الله القهيوي، زياد كامل اللالا، و بلال محمود الوادي. (2013). جودة المعلومات والذكاء الاستراتيجي في بناء المنظمات المعاصرة. الأردن: الحامد للنشر والتوزيع.

– محمد محمود مكاوي. (2009). البيئة الرقمية :بين سلبيات الواقع وآمال المستقبل. مصر: دار الكتب والوثائق القومية.

2.1.5. المقالات:

– سليمان صادق درمان. (2003). فاعلية نظام المخابرات التسويقية في اتخاذ القرارات التسويقية،. *تنمية الرافدين ، 25* (72)، الصفحات 01-16.

– سندس نوري شكر. (2010). الأساليب الحديثة في تدقيق ومراجعة نظم المعلومات. ،مجلة العلوم الاقتصادية و الإدارية ، 16 (59)، الصفحات 222-235.

– عبد المجيد قدي، و رتيبة نحاسية. (2014). أدوات البحث عبر الويب في خدمة اليقظة الإستراتيجية للمؤسسات. مجلة علوم الاقتصاد والتسيير والادارة ، 2 (29)، الصفحات 217-240.

– عمر ولد عابد، و أمين علواطي. (2017). آليات تطبيق اليقظة الإستراتيجية بالمؤسسات الاقتصادية الجزائرية "نموذج مقترح" دراسة تطبيقية بمؤسسة الإسمنت بالشلف. الألكاديمية للدراسات الإجتماعية والإنسانية (17)، الصفحات 3-15.

– فاطمة بوداود. (2019). دور الانترنت في إرساء اليقظة الإستراتيجية بمؤسسة اتصالات الجزائر– وهران. مجلة أبحاث إقتصادية وإدارية ، 13 (01)، الصفحات 129–158.

– نايف صلاح الغمري. (مارس, 2012). أمن المعلومات وآثاره عل أداء المصارف التجارية– دراسة استطلاعية على محافظة جدة. *مجلة الأندلس للعلوم الاجتماعية والتطبيقية ، 5* (8)، الصفحات 113–183.

3.1.5.المداخلات:

-حمد عبد الدايم. (18–20 أفريل, 2004). أمن الشبكات الخاصة،مداخلة مقدمة ضمن ندوة مراجعة وتدقيق نظم المعلومات، .القاهرة:المنظمة العربية للتنمية الإدارية– جامعة الدول العربية.

-عبد ذياب العجيلي. (18–20 أفريل, 2004). الأساليب الحديثة في تدقيق ومراجعة نظم المعلومات . ندوة مراجعة وتدقيق نظم المعلومات، المنظمة العربية للتنمية الإدارية– جامعة الدول العربية.مصر.

-محمد محمد الألفي. (03–07 جوان, 2007). الحماية القانونية لقواعد البيانات في نظم المعلومات،ندوة أمن وحكاية نظم المعلومات، المنظمة العربية للتنمية الإدارية–جامعة الدول العربية،مصر.

-ممدوح الشحات صقر. (3–7 جوان, 2007). أمن المعلومات. ندوة أمن وحكاية نظم المعلومات، المنظمة العربية للتنمية الإدارية–جامعة الدول العربية،مصر.

2.5. المراجع باللغة الأجنبية:

1.2.5. الكتب:

- Guichardaz, P., Lointier, P., & Rosé, P. (1999). L'Infoguerre:Stratégies de contre-intelligence économique pour les entreprises. France: DUNOD.

- Jakobiak, F. (2004). L'intelligence économique :la comprendre -l'implante- l'utiliser. France: Edition D'organisation.

- Lendrevie, J., Levy, J., & Lindon, D. (2006). Mercator (éd. 8e édition). France: Dunod.

- Löning, H., Malleret, V., Méric, J., Pesqueux, Y., & Sole, A. (2008). Le contrôle de gestion :organisation ;outils et pratique (éd. 8e édition). France: Dunod.

2.2.5. الرسائل والأطروحات:

- Bisson, C. (2003). Application de méthodes et mise en place d'outils d'intelligence compétitive au sein d'une pme high-tech(these pour obtenir le grade de docteur en science). Université de droit et d'économie et des sciencedAix marseille.France.

- Lopez da Silva, A. (2002). L'information et l 'entreprise : des savoir à partager et à capitaliser-méthodes.outils et application à la veille- (thèse pour obtenir le grade de docteur en sciences).Université de droit, d'économie et des sciences d'Aix Marseille.France.

3.2.5. المقالات:

- Asselin, C. (2008). comment faire de la veille image? ,Documentaliste-Sciences de l'information , 45 (2008/4), pp. 58-69.

- Ayachi, H. (2007). l'adéquation entre le systèm d'information et la vielle stratégique dan une activité de construction de sens. Management et Avenir , 12 (2007/2), pp. 49-66.

- Bergeron, P. (1995). observation sur le processus de vielle et les obstacles à sa pratique dans les organisations. Argus , 03 (24), pp. 17-22.

- Deschamps, C. (2008). Comment bien utiliser agrégateurs de flux RSS et agents de surviellance?, Documentaliste-Sciences de l'information , 45 (2008/4), pp. 46-57.

- Janissek-Muniz, R., Freitas, H., & Lesca, H. (2006). veille anticipative stratégique, intelligence (VAS-IC): usage innovant du sute web pour la provocation d'informations terrain. la revue des sciences de gestion , 2018 (2006/2), pp. 19-30

4.2.5.المداخلات:

- Alexandre-Leclair, L. (2001, octobre 15-19). La sûreté économique comme stratégie de contre intelligence économique , IRIT – DELTA VEILLE, COLLOQUE VEILLE STRATEGIQUE SCIENTIFIQUE & TECHNOLOGIQUE , Barcelone.
- Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., et al. (2011). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-137 (Accessed April 13, 2022).
-Żywiołek, J. (2018,July 31). Monitoring of information security system elements in the metallurgical enterprises. *12th International Conference Quality Production Improvement.* MATEC Web Conf., 183 (2018) 01007.DOI: https://doi.org/10.1051/matecconf/201818301007.

5.2.5.التقارير:

- AFFRES, L., BAILLY, R., BREITNER, S., CHABOUD, C., D'ESTAINTOT, R., DE LASTOURS, S., et al. (2003). Entreprises et intelligence économique :quelle place pour la puissance publique ?. INSTITUT DES HAUTES ETUDES DE LA SECURITE INTERIEURE.France