أمن الوثائق والمعلومات الإلكترونية واستراتيجيات حفظها في الأرضية الرقمية لقطاع التربية

دراسة حالة النظام الفرعي لمديرية التربية لولاية قسنطينة

Electronic files and data security and strategies for storage on the education sector digital platform

Case study of the sub-system of the department of education in the Wilaya of Constantine

بليان مسعود [1]

طالب دكتوراه جامعة قسنطينة 02 عبد الحميد مهري

Messaoud.Beliane@Univ-Constantine2.Dz

عكنوش نبيل

جامعة قسنطينة 02 عبد الحميد مهري

Nabil.Aknouche@Univ-Constantine2.Dz

تاريخ الوصول 2020/09/23 القبول 2021/04/05 النشر على الخط 2021/09/30

Received 23/09/2020 Accepted 05/04/2021 Published online 30/09/2021

ملخص:

ساهمت التقنية الحديثة في سرعة انتاج المعلومات وسهولة تداولها مستغلة في ذلك خدمات شبكة الانترنيت الامر الدي أدى إلى فتح منافذ على المؤسسات سهلت اختراق الأجهزة وقرصنة الأنظمة ومن ثم تحريف محتوى الوثائق الالكترونية والعبث بمحتوياتها وبالتالي المساس بالحياة الشخصية للأفراد أو الهيئات. نهدف من خلال دراستنا إلى عرض واقع أمن الوثائق والمعلومات الخاصة بالمنتمين لقطاع التربية والمتاحة عبر المنصة الرقمية، وتبيان الاستراتيجيات والتدابير المعتمدة من طرف الهيئة الوصية للعناية بها وحمايتها من مختلف المخاطر التي تتربص بها، أيضا بغية التعرف على التقنيات والوسائل والأدوات المجهزة للتصدي لهده الاخطار مهما كانت أنواعها ومسبباتها، وقد توصلت نتائج البحث أن الوزارة الوصية اقرت استراتيجية مكتوبة بغرض حماية الحسابات الإلكترونية الشخصية للمستخدمين وفقا للمنشور رقم: 2018/230، كما أصدرت قبله وتحديدا سنة 2017 المنشور رقم 1098 بتاريخ: 25 ماي 2017 يخص التدابير الوقائية ضد الهجومات الالكترونية) بخصوص فيروس (Ransomware)

---

[1] – المؤلف المرسل: بليان مسعود البريد الإلكتروني: Messaoud.Beliane@Univ-Constantine2.Dz

الكلمات المفتاحية: أمن المعلومات والوثائق الإلكترونية – الحفظ الرقمي – الأرضية الرقمية الوطنية – مديرية التربية لولاية قسنطينة – الجزائر.

Abstract:

The new technologies have contributed to the rapid production and easy flow of information, taking advantage of the services offered by the Internet; this has opened gaps in companies and thus facilitates the hacking of devices and systems and consequently the alteration of electronic files and its content which will lead to a breach of the private life of individuals or organizations.

Our study aims to present the reality of files and data security relating to the affiliates of the education sector on the digital platform; and to determine the strategies and measures adopted by the tutorship to monitor it and protect it from the various risks to which it is also exposed in order to identify the techniques, means and tools for dealing with such threats, whatever the type and the causes.

The results of the research showed that the supervising ministry has adopted a written strategy to protect users' personal electronic accounts in accordance with Circular 230/2018. It also issued before it, specifically in 2017، circular number 1098 dated May 25, 2017, on the prevention of cyber-attacks involving the virus (Ransomware), and a firewall was also used to counter various attacks threatening data security.

Keywords: Data security and Electronic files - Digital storage - Digital platform National - Department of Education in the Wilaya of Constantine - Algeria.

1. مقدمة:

إن من أبرز مظاهر التطور التكنولوجي الحالي كونه أصبح من أنجع وسائل التواصل والاتصال بين الأمم والشعوب كونه يتيح الفرصة للانفتاح على العالم الخارجي مهما بعدت الأماكن وطالت المسافات مستغلا في ذلك شبكات المعلومات والأنترنيت، هدا الأخير الذي بالرغم من المزايا التي يقمها والتي لا تعد ولا تحصى إلا أنه سلاح ذو حدين إدا ما ساء استخدامه، ودلك لأنه يسمح بفتح منافذ تؤدي لاختراق الأجهزة وقرصنة الأنظمة ومن ثم تحريف محتوى الوثائق الالكترونية والعبث بمحتوياتها وبالتالي المساس بالحياة الشخصية للأفراد أو الهيئات. ومنه انبثق علم جديد يصطلح على تسميته أمن المعلومات وهو ذلك العلم

الذي يبحث في استراتيجيات ونظريات توفير الحماية اللازمة للمعلومات من الأخطار التي تهددها باختلاف نوعها أو مصدرها ومن أنشطة الاعتداء عليها [1].

لذلك أصبح من واجب الهيئات والمنظمات المتواجدة في البيئة الرقمية والتي تستخدم الأنظمة الألية والمنصات الرقمية في تعاملاتها وأنشطتها وضع استراتيجية أمنية محكمة على عدة مستويات من أجل تأمين معلومتها ووثائقها من مختلف الأخطار التي قد تتعرض لها على سبيل المثال لا الحصر تلك المحاولات الخارجية أو الداخلية للاختراق، القرصنة، أو الاعتداءات الإلكترونية ناهيك عن الإشكاليات المتعلقة بالحفظ وديمومة المعلومات الرقمية.

وزارة التربية الوطنية أنموذجا لهده المؤسسات الدولة الجزائرية صممت منصة رقمية مند 2015 أطلق عليها اسم " الأرضية الرقمية لقطاع التربية الوطنية " وتحوي هده الأخيرة كل المعلومات والوثائق والنشاطات والخدمات الخاصة بقطاع التربية مقسمة إلى ثلاثة محاور أساسية هي: نظام تسيير المستخدمين، نظام تسيير التلاميذ، ونظام تسيير الهياكل والسكنات الوظيفية.

تأسيسا لما سبق ذكره نطرح التساؤل التالي:

ما هو واقع المخطط الأمني المسطر لحماية النظام المعلوماتي وحفظ مخرجاته؟

ومنه يمكن طرح الأسئلة الفرعية التالية:

- ما هو أمن الوثائق والمعلومات؟ وما أبرز المخاطر المهددة له؟ وفيما تتمثل المبادئ الأساسية التي يرتكز
عليها؟
- فيما تتمثل استراتيجية الحفظ الرقمي لمخرجات النظام بهدف إطالة عمرها
- هل تم إشراك الأرشيفي عند تصميم وتنفيذ المخطط الأمني؟
- كيف يتم مجابهة تحديات أمن المعلومات؟ وما الأدوات / التقنيات والتدابير المتبعة حيال دلك؟
- هل توجد سياسة أمنية لحفظ وحماية المعلومات مستقبلا على المدى البعيد؟

---

[1] - مصطفى البكري، يوسف علي الشيخ، أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلى مكتبتي النيلين وجامعة وادي النيل Qscience proceeding.vol3.The SLA-AGC. 23rd Annual conference.2017 Available on : https://doi.org/10.5339/qproc.2017.gsla.3

تهدف دراستنا لتحقيق جملة من الأهداف أبرزها ما يلي:

- استكشاف واقع امن المعلومات وحمايتها بالأرضية الرقمية لقطاع التربية الوطنية
- معرفة التدابير والإجراءات المتبعة عند تقييد المعلومات والبيانات في الأرضية الرقمية بغرض تأمينها
- التعرف على والقوانين والتشريعات التي تضمن حماية الوثائق والمعلومات الالكترونية عند الاتاحة
- ابراز الدور الدي لعبه الارشيفي ضمن الاستراتيجية المسطرة من قبل الهيئة الوصية حول أمن المعلومات وحفظها على المدى البعيد.
- معرفة المخططات الأمنية المطبقة المضادة الهجمات التي تتعرض لها الأرضية الرقمية
- محاولة الكشف عن مواطن القوة والضعف لنظام الأمن المعتمد وتقديم اقتراحات مناسبة

كما تستمد دراستنا أهميتها من أهمية الموضوع الذي تعالجه وهو أمن الوثائق والمعلومات الإلكترونية لأن:

- موضوع أمن المعلومات الإلكترونية وحمايتها يكتسي أهمية كبيرة باعتباره وليد عصر التقدم التكنولوجي الراهن.
- الحجم الكبير للمنظومة التربوية وقطاع التربية ككل واحتوائها على معلومات تخص الأفراد وجب حمايتها.
- واقع الحفظ الرقمي واستراتيجياته في مشروع الأرضية الرقمية لقطاع التربية باعتباره العمود الفقري لأي مشروع رقمنة.
- التعرف على خدمات المعلومات الالكترونية المتاحة عبر الأرضية الرقمية ومستويات تأمينها.
- الوقوف على الاستراتيجية المسطرة من طرف الهيئة الوصية لحماية وتأمين الأرضية الرقمية.

حيث يعتر المنهج هو اللبنة الأولى لانطلاق أي دراسة علمية فهو عبارة عن سلسلة من المراحل المتتالية التي ينبغي إتباعها بكيفية منسقة ومنظمة[1]. اعتمدنا على منهج دراسة الحالة والمنهج الوصفي لأنه الأنسب لدراستنا إذ يوفر مجموع الأدوات التي تمكن من تجميع المعلومات من الظاهرة محل الدراسة بغرض وصفها ومناقشتها وتحليلها. ويتمثل المجتمع الأصلي لهذه الدراسة في فريق مشروع الرقمنة بمديرية التربية لولاية قسنطينة المتكون من تسعة عشرة فردا (19) تحت اشراف مدير مشروع الرقمنة الدي اجرينا معه المقابلة.

---

[1]- أنجرس، موريس، منهجية البحث العلمي في العلوم الإنسانية: تدريبات علمية. ط02، الجزائر، دار القصبة،2006، ص33.

ومن أجل تجميع البيانات استخدمنا المقابلة كأداة أولى أساسية، ثم الملاحظة كأداة إضافية، فالمقابلة تستعمل إزاء الأفراد الذين تم سحبهم بكيفية منعزلة، غير أنها تستعمل في بعض الحالات إزاء المجموعات من أجل استجوابهم بطريقة نصف موجهة والقيام بسحب عينة كيفية بهدف التعرف بعمق على المستجوبين[1]، في دراستنا قمنا بإجراء مقابلة مع مدير مشروع الرقمنة بمديرية التربية لولاية قسنطينة باعتباره المسؤول الأول حول تسيير وإدارة المشروع بعد مدير التربية. احتوت المقابلة على**30 سؤالا** موزعة عبر ستة محاور، حيث جاء المحور الأول للتعريف بمصطلحات ومفاهيم عامة تخص الأمن المعلوماتي، أما المحور الثاني فتناولنا من خلاله فكرة وضع الأرضية الرقمية وظروف ذلك، ثم في المحور الثالث تطرقنا إلى كل ما يتعلق بتصميم وبناء أرضية رقمية أمنة للمعلومات، المحور الرابع خصصناه لإبراز عمليات تسجيل وتقييد البيانات في الأرضية الرقمية والاحتياطات المتبعة لضمان تأمينها، أما المحور الخامس فتطرقنا من خلاله الى مختلف الخدمات والوثائق التي تتيحها الأرضية الرقمية والأدوات والتدابير المتوفرة لحمايتها وحفظها على المدى البعيد، وختمنا المقابلة بمحاولة معرفة ما إدا تم اقرار استراتيجية أمنية مستقبلية لتامين وحماية المعلومات وحفظها في البيئة الرقمية على المدى الطويل. أما الملاحظة فهي فعل فحص الظاهرة بكل اهتمام وعناية حيث تسمح بما لها من جاذبية باكتشاف وفهم بعض جوانب الظواهر التي مازالت إلى حد الآن مبهمة، والتي كانت في البداية خالية من أية فائدة. اعتمدنا في دراستنا على الملاحظة المكشوفة التي هي حالة يعرف فيها الأشخاص الملاحظين أنهم محل ملاحظة[2]. حيث عمدنا باستخدام هذا النوع من الملاحظة نظرا لما له من أهمية في فهم الظاهرة محل البحث فهما دقيقًا، لأنها مكنتنا من معاينة مشروع النظام الفرعي لمشروع الأرضية الرقمية بمديرية التربية لولاية قسنطينة وبنظرة موضوعية بعيدا عن أي لبس ومشاهدة مراحل المشروع وخطواته مند انطلاقه بما في دلك الشق الأمني للمشروع.

الدراسات السابقة يعرفها شعبا عبد العزيز خليفة على أنها " البحوث العلمية التي أعدت من قبل في نفس نقطة البحث"[3] حيث حاولنا الاطلاع على الدراسات التي تناولت نفس موضوعنا والمواضيع ذات الصلة.

---

[2]-أنجرس موريس، المرجع نفسه. ص197.

[2]-أنجرس موريس، المرجع نفسه. ص 187-189

[2]-خليفة، شعبان عبد العزيز، المحاورات في مناهج البحث في علم المكتبات والمعلومات. مصر: الدار المصرية اللبنانية، 1997، ص101.

الدراسة الأولى باللغة العربية تحت عنوان: " **استراتيجية أمن المعلومات** "[1] حيث تطرقت الباحثة في دراستها إلى مجموعة من المفاهيم المتعلقة بأمن المعلومات كمفهوم أمن المعلومات، أهمية أمن المعلومات، أهداف وأركان أمن المعلومات، ثم تطرقت إلى المخاطر التي تتعرض لها العمليات الإلكترونية وكيفية الحد من تلك المخاطر، وانتقلت الى طريقة صياغة استراتيجية المعلومات داخل المنظمة وخطط بنائها بغرض إعطاء الخطوة الصحيحة لتطبيق الحماية الأمنية للمعلومات.

هدفت الدراسة الى:

- التأكيد على أن أهمية أمن المعلومات للمنظمات هي حاجة ماسة وضرورية
- تثقيف العاملين بأهمية الأمن في المنظمة وتدريبهم على ذلك
- تقديم استنتاجات وتوصيات يمكن من خلالها مساعدة المنظمة على تبني استراتيجية أمنية وتطبيقاتها، لمواجهة التهديدات والمخاطر بكفاءة وفاعلية.

أما منهج البحث الذي اعتمدت عليه فهو المنهج الوصفي التحليلي، وذلك من خلال الاستعانة بالمصادر العلمية ذات العلاقة بالموضوع، والوسائل الالكترونية الأخرى.

توصلت الدراسة إلى مجموعة من النتائج أبرزها:

- تواجه المنظمات مخاطر أمنية من مصادر كثيرة، منها الأخطاء البشرية، الأخطار البيئية، وأخيرا الجرائم المحوسبة؛ ولذلك يجب وضع استراتيجية أمنية فعالة لمواجهتها
- إن الهدف من صياغة استراتيجية الأمن وتنفيذها هو تحسين توافر المعلومات وتكاملها، وخصوصيتها داخل وخارج المنظمة.
- عند بناء استراتيجية أمنية يجب تحديد الإجابة عن التساؤلات الثلاثة الرئيسة: ماذا أريد أن أحمي؟ من ماذا أحمي المعلومات؟ كيف أحمي المعلومات؟
- إن أمن المعلومات يحتاج إلى استراتيجية قوية؛ بهدف حماية البنية التحتية والتصدي للتهديدات وعليه يمكن حصر التوصيات في النقاط الآتية:

---

[3] – قدايفية أمينة، استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، المجلد 06، العدد01، متاح على المنصة الوطنية للمجلات الجزائرية ASJP على الرابط : https://www.asjp.cerist.dz/en/article/31120 تاريخ الزيارة: 2019/02/24.

- العمل على حماية المعلومات عند تخزينها، وذلك بتشفيرها، أو وضع كلمة مرور خاصة عند الحفاظ والتخزين على مختلف الوسائط حتى لا يتمكن أحد من اختراقها
- أهمية التوعية ونشر ثقافة أمن المعلومات بين جميع الموظفين تتلخص في الآتي:
- إنشاء دائرة خاصة بأمن المعلومات تزود بإطارات مؤهلة لإدارتها، ومنحها صلاحيات قوية تؤهلها لتطوير وتطبيق السياسات الأمنية، وذلك بدعم الإدارة العليا لها.
- رفع الوعي الأمني لدى جميع موظفي المنظمة على اختلاف مستوياتهم وذلك بعمل دورات تدريبية خاصة بهم.
- إضافة ميزة إغلاق رقم المستخدم بعد ثلاث محاولات فاشلة وذلك لمنع محاولة الدخول على النظام بتخمين كلمة السر
- لتطبيق سياسة صارمة تجاه كلمة السر يجب وضع مواصفات قياسية لكلمة السر، من حيث عدد الحروف وتنوعها بين الحروف والأرقام والرموز، وعدم تكرار الحروف، وعدم إعادة استخدام الكلمة نفسها حتى انقضاء فترة من الزمن، وليكن عاماً مثلا، وطلب تغيير الكلمة بصورة دورية وتضمين هذه المواصفات في البرامج التطبيقية لفارض السياسة على جميع المستخدمين.

الدراسة الثانية: " **أمن المعلومات بلغة ميسرة** " [1] وهو عبارة عن كتاب استهل فيه الباحثان الحديث عن شبكة الأنترنيت وبعض الجرائم المتعلقة بأمن المعلومات بصفة عامة، ثم عرجا بالحديث عن الهندسة الاجتماعية تعريفها، أهميتها، الجوانب المتعلقة بها، وطرق الهجمات الالكترونية باستخدام الهندسة الاجتماعية، وفي العنصر الدي يليه تناولا كلمات المرور من حيث التعريف والأهمية والاخطار المترتبة عن سوء استخدامها، ثم تطرقا الى البرامج الخبيثة أنواعها ودوافع تطويرها، طرق الإصابة بها والحلول للوقاية منها، وأيضا الفيروسات من حيث الأنواع وطرق العلاج منها.

وفي المحور الدي يليه قاما بالحديث عن وسائل الحماية وتوفير الأمن للمعلومات ومنها أحصنة طروادة، جدران الحماية، تحويل العناوين الرقمية، التحديث الانتقائي، التشفير، كما تطرقا أيضا إلى جانب دو علاقة

---

[1]_ أمن المعلومات بلغة ميسرة، القحطاني محمد عبد الله علي، خالد سليمان الغثبر، مركز التميز لأمن المعلومات: الرياض، 2009 متاح على الخط : books-library.online/free-1917333-download تاريخ الزيارة: 2019/02/26.

بوسائل الحماية الدي يتمثل في طمس البيانات والمشاركة في الملفات والمجلدات، التخزين الاحتياطي، والبريد الإلكتروني. كما تناول الكتاب أيضا جوانب متفرقة لكن لها علاقة بأمن المعلومات في البيئة الرقمية تمثلت في:

- التسوق الامن، السرية على الأنترنيث، ميكروسوفت للأنترنيت، المساعدات الرقمية الشخصية، البلوتوت والحواسيب المحمولة.

أما الدراسات باللغات الأجنبية فنستهلها بدراسة تحت عنوان: **Employees' adherence to information security policies: An exploratory field study**[1] حيث يرى الباحثون أن التهديد الرئيسي لأمن المعلومات يأتي من الموظفين الذين لا يلتزمون بسياسات أمن المعلومات. حيث قاموا بتطوير نموذجًا جديدًا يستند إلى نظريات متعددة يشرح التزام الموظفين بسياسات الأمان. يجمع النموذج بين عناصر من: (نظرية دافع الحماية، ونظرية الفعل العقلاني، ونظرية التقييم المعرفي). حيث تم التحقق من النموذج المقترح من خلال توزيعه على عينة من 669 فردًا من أربع شركات في فنلندا.

وأظهرت النتائج أن قوة التهديدات المحتملة على أمن المعلومات، والتزام الموظفين بتطبيق سياسات أمن المعلومات، الاستهانة بضعف التهديدات الأمنية المحتملة، وموقف الموظفين تجاه الامتثال لسياسات أمن المعلومات، والمعايير الاجتماعية تجاه الامتثال لهذه السياسات كان لها تأثير كبير وإيجابي على نية الموظفين في الامتثال والتقيد لسياسات أمن المعلومات. وكان للنية في الامتثال لسياسات أمن المعلومات أيضا أثر كبير على الامتثال الفعلي لهذه السياسات. ويجب على المديرين رفيعي المستوى أن يحذروا الموظفين من أهمية أمن المعلومات ولم لا من الضروري تنفيذ هذه السياسات. وبالإضافة إلى ذلك يجب تزويد الموظفين بالتعليم الأمني والتدريب العملي.

---

[1] - Siponen, M., Mahmoud, M. A., & Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2),2014, 217-224.

والدراسة الثانية تحت عنوان: [1] **Cryptography & Security** تقرير ندوة مقدم من طرف Vibjan Kolapati للحصول على درجة بكالوريوس في التكنولوجيا(B.Tech) في علوم الكمبيوتر و الهندسة كلية الهندسة جامعة Kochi للعلوم والتكنولوجيا.

تناولت الدراسة بشكل عام التشفير ومدى أهمية في أمن وحماية المعلومات، حيث استهل الباحث دراسته بإبراز أنواع التشفير المعتمدة في تكويد البيانات والمعلومات والمتمثلة في: الرموز، سجلات الرموز، الشفرات. ثم انتقل في المحور الثاني للحديث عن شفرات الحواسيب والخدمات الأمن وطرق مواجهة التهديدات الأمنية. وفي المحور الموالي انتقل الى توضيح اليات الأمن المتمثلة في: التوقيعات الرقمية، الخوارزميات المجزئة. واختم الباحث دراسته بأهم التطبيقات المعتمدة في التشفير، ومن النتائج التي توصلت اليها الدراسة ان التشفير يمتلك درجة عالية من التعقيد لدلك وجبت الحاجة إلى التفاعل السليم للتشفير والتحليل المشفر. وينشأ ذلك من حقيقة أنه في غياب متطلبات الاتصالات الحقيقية أصبح من السهل اقتراح نظام غير قابل لفتح التشفير، وان العديد من التصميمات الأكاديمية معقدة للغاية لدرجة أن المحلل المشفر لا يعرف من أين يبدأ معناه فضح العيوب في هذه التصاميم أصعب بكثير من تصميمها في البداية، والنتيجة أن العملية التنافسية التي تعد دافعًا قويًا في البحث الأكاديمي، لا يمكن أن تترسخ في العديد من التطبيقات مفيدة في الوقت الفعلي وفي الحياة اليومية والتي يتم تنفيذها عن طريق التشفير من خلال المفهوم الضمني أو الصريح لها، على سبيل المثال النظام المصرفي، ATM للبطاقات، البطاقات الذكية، تقنية الشريط المغناطيسي، وكالة الأمن القومي (NSA) ، ومع المواد المجهزة تجهيزًا جيدًا والتجارة الإلكترونية والاقتصاد والمعلومات التجارية وأنظمة التشغيل وقواعد البيانات وأخيرًا فيSystem Protection وبهذه الطريقة يكون للتشفير العديد من الأدوار والعديد من التطبيقات.

---

[1]- Kolapati, V , *Cryptography and Security*. Disponible sur : mailto:http://dspace.cusat.ac.in/jspui/bitstream/123456789/2628/1/Cryptography%20and%20Security.pdf visite le : 14/03/2020.

2. أمن المعلومات والوثائق الإلكترونية:

1.2 تعريف أمن المعلومات: هناك عدة تعاريف تناولت مفهوم أمن المعلومات، نذكر منها ما يلي :

*يعبر عن أمن المعلومات بأنه" الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية".

أمن المعلومات هو كذلك" مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال"[1]

* عرف كلا من Mathod وWhitman أمن المعلومات في كتابهما " مبادئ أمن المعلومات " بأنه (الحفاظ على سرية وتوفر وسلامة المعلومات كأصل في مراحل المعالجة والحفظ والنقل، ويتحقق دلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب، ويرى كلاهما أن تحقيق إدارة أمن نظم المعلومات يشمل المكونات التالية:

- الأمن المادي: بما يشمله من مصادر وممتلكات ومباني لمنع الوصول غير المشروع
- أمن الأفراد: لحماية الافراد والمجموعات الذين لهم حق الوصول للمعلومات.
- أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون
- أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى.
- أمن الشبكات: لحماية مكونات الشبكة والتراسل والمحتويات.
- أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات[2]

من خلال التعاريف السابقة يتضح أن أمن المعلومات مصطلح يضم في طياته عمليات واجراءات شاملة لحماية الوسائل والاجهزة والكيانات الرقمية المتوفرة في المنظمة عن طرق وضع خطة ومنهجية محكمة وضرورة الالتزام بتطبيقها.

---

[1] – قدايفية أمينة، المرجع نفسه، ص160-178

[2] – فيلالي أسماء، شليل عبد اللطيف، تهديدات أمن المعلومات وسبل التصدي لها. مجلة البشائر الاقتصادية (المجلد الرابع، العدد 03)، 2017، ص 163-177

* عبارة عن مجموعة من العمليات والمعايير والأليات التي تصمم وتنفذ لأغراض حماية المعلومات من الوصول الغير مشروع من أجل إساءة الاستخدام أو التخريب[1]

من خلال هدا التعريف يتضح أنه مرتبط بالولوج للمعلومات بطرق غير قانونية وشرعية والخطط المنتهجة للحد من هده الظاهرة.

2.2 المخاطر والاعتداءات في بيئة الأعمال:

وتشمل مواطن الاعتداء على سلامة المعلومات العناصر الأتية:

1.2.2 الأجهزة: كافة المعدات والأدوات المادية التي تتكون منها النظم كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.

2.2.2 البرامج: وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال وهي إما مستقلة عن النظام أو مخزنة فيه.

3.2.2 المعطيات: وهي الدم الحي للأنظمة وما سيكون محلا لجرائم الكمبيوتر كما سنرى، وتتمثل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظام. والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين الخارجية.

4.2.2 الاتصالات: وتشمل شبكات الاتصال التي تربط الأجهزة التقنية ببعضها البعض محليا ودوليا، وتتيح فرصة اختراق النظم عبرها، وهي بذاتها محل اعتداء وموطن من مواطن الخطر الحقيقي.

5.2.2 المورد البشري: ومحور الخطر هو الإنسان، سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراك هدا الشخص حدود صلاحياته، وادراكه أليات التعامل مع الخطر وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية هي مسائل رئيسية يعنى بها نظام الأمن الشامل وتحديده في بيئة العمل المرتكزة على نظم الكمبيوتر وقواعد البيانات [2].

ومن الفروق الجوهرية بين المخاطر التي تتعرض لها المعلومات المخزنة في أجهزة الحاسوب وتلك التي تتعرض لها المعلومات المكتوبة على الورق وتتمثل في:

---

[1] - Campbell, T. *Practical Information Security Management*. Apress,2017

[2]- قذايفية أمينة، مرجع سابق، ص 166-167.

– خطر كشف المعلومات السرية: السطو على المعلومات قد ينتج عنه إطلاع المهاجم على معلومات ما كان ينبغي له الاطلاع عليه، وهدا لكشف معلومات كان مالكوها يرغبون في حفظها بسرية وهدا الصنف يقع على المعلومات المخزنة على أوراق، كما يقع على تلك المخزنة في الحواسيب على حد سواء.

– خطر حرمان مالك المعلومات من الوصول إليها عند الحاجة: إن السطو على المعلومات المخزنة على الورق قد ينجم عنه حرمان صاحب هده المعلومات منها إدا كانت النسخة المسروقة هي النسخة الوحيدة. كما أن هدا النوع من الأخطار يمكن ان يحدق بالمعلومات المخزنة في أجهزة الحاسوب.

– خطر تغيير المعلومات: المعلومة المخزنة على الورق تتمتع بخاصية مهمة هي أن أي تغيير عليها يسهل للإنسان – في أغلب الأحيان – ملاحظته ولدلك فإنه يصعب على من يسطو ان يقوم بتغيير تلك البيانات دون ترك أثار تدل على دلك. أما البيانات المخزنة على وسائط مغناطيسية فإن العبث بها دون ترك أثار تدل على وقوع دلك يعد أمرا ميسورا [1].

ومن أبرز مظاهر التهديد على أمن المعلومات التي تتعرض لها المؤسسات والهيئات ما يلي: [2]

- سرقة البيانات
- انتهاك السرية والخصوصية
- فقد تكامل البيانات
- تعطل النظام

3. استراتيجيات وطرق أمن وحماية المعلومات:

1.3 استراتيجية أمن المعلومات حيث تتكون الاستراتيجية من:

1.1.3 الاستراتيجية نفسها: والتي توثق لحماية لدوافع حماية المؤسسة لبياناتها وما هي هذه البيانات، والتي يمكن بناؤها في الخطوات التالية:

- تحديد المادة أو الموضوع محل الاهتمام والمراد عمل استراتيجية له.

---

[1] – الغثبر خالد بن سليمان، القحطاني، محمد بن عبد الله، مرجع سابق، ص12.11

[2] – الصاحب، محمود حسن، سياسة أمن المعلومات في الجامعات: حالة دراسية (مجلة سيبرارين ع33. ديسمبر 2013) متاح على: mailto:http//www.cybrarians.info/journal/n…o-secuirty.htm الزيارة بتاريخ: 2020/03/21.

- ماهي العمليات والنشاطات المسموح بها المستخدمين وما هي النشاطات الغير مسموح بها؟ ولمن من المستخدمين؟
- تحديد الأشخاص (المستخدمين) المتأثرين بهذه الاستراتيجية
- تحديد كيفية تطبيق الاستراتيجية في بيئة المنظمة
- تحديد المخاطر المتوقعة في البيئة المحددة
- تحديد وتصنيف البيانات وموارد النظام
- تحديد خدمات الأمن الأساسية في بيئة المنظمة
- تحديد قائمة السياسات التي أ نشئت
- إنشاء تحليل لانسياب البيانات المصنفة منذ مرحلة الإنشاء وحتى الحذف من النظام
- توثيق الاستراتيجية

2.1.3 المعايير: وهي توثق لماهية المقاصد المنشودة لتطبيق وإدارة أمن المعلومات.

3.1.3 الإجراءات: وهي توثق للكيفية التي تنجز بها المنظمة المتطلبات المفروضة بالمعايير والاستراتيجيات، وهي الأدوات التي تحول بها السياسات إلى أحداث وعمليات بعد إنشاء السياسات يجب توزيعها على كل مستويات صلاحية السياسات يجب تعهدها بالمراجعة المستمرة، ودلك بتحديث أليالها وأدواتها، ويجب عكس التغييرات في بيئة عمل المنظمة على سياسات التأمين أولا بأول[1] الهيكل التنظيمي (مستخدمين، موظفين، الإدارة، الزبائن، الاستشاريين. ولضمان

2.3 طرق حماية المعلومات:

1.2.3 الحماية التقنية لنظم المعلومات وبرامجها: وتشمل حماية استخدام كل البرامج المتاحة والتي توفر حماية للمعلومات المتداولة عبر شبكات المعلومات أو المخزنة في أجهزة الحواسيب، وهي كما يلي:

1.1.2.3 برامج مكافحة الفيروسات: هي برمجيات تستخدم لاكتشاف وإزالة كافة أنواع البرمجيات الضارة والخبيثة والعمل على محوها تماما من النظام لما لهده البرمجيات م تهديدات قد تؤثر على أمن المعلومات التي تضمها المنظمة.

---

[1] – قدايفية أمينة، مرجع سابق، ص174.173

2.1.2.3 جدار النار: هو كل أله موضوعة في شبكة معلوماتية قادرة على المتواصلات الداخلة والخارجة

3.1.2.3 التشفير: هو مجموع التقنيات التي تهدف إلى تحويل بفعل اتفاقيات سرية، معلومات أو إشارات واضحة إلى معلومات أو إشارات غير واضحة من أجل تحقيق الفرضية المعاكسة عن طريق وسائل مادية أو برامج متخصصة لذلك [1]

2.2.3 مراقبة الدخول وأنظمة كشف التدخل: وتشمل العناصر التالية:

1.2.2.3 مراقبة الدخول: مراقبة الدخول هي كل السياسات والاجراءات المتخذة من قبل مؤسسة من أجل ايقاف أو إعاقة الدخول للأنظمة من قبل أشخاص ممنوعين، والدخول إلى النظام يتطلب التعريف بالهوية + التحقق من الهوية.

2.2.2.3 أنظمة كشف التدخل :أنظمة كشف التدخل هي عبارة عن أدوات للمراقبة مستمرة موضوعة في أماكن أو نقاط الدخول الأكثر حساسية لشبكات المؤسسة من أجل كشف التدخلات، ومن ثم يطلق النظام إنذار في وقت حقيقي في حال حدث مريب أو غير عادي [2]

3.2.2.3 تأمين وحماية ممتلكات المؤسسة المادية: هي كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها مثل: الأقفال والحواجز والغرف المحصنة وغيرها من الوسائل التي تقوم على حماية الأجهزة الحساسة من العبث أو التخريب [3]. يمكن أن نقسم متحكمات الأمن المستخدمة لإدارة الأمن المادي إلى ثلاث مجموعات أساسية [4]

– متحكمات الأمن المادي الإدارية: وتتمثل في بناء واختيار موقع وإدارة الموقع وضبط المستخدمين والتدريب والاطلاع والاستجابة لحالات الطوارئ.

---

[1]- Léopold. E, & Lhoste. S, la sécurité informatique. 3éme édition ،2007

[2]- فيلالي أسماء، شليل عبد اللطيف، مرجع سابق، ص170

[1] -حسني علي قاسم الشمالي، أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية في البنوك العاملة في الأردن. إدارة أعمال، كلية توليدو الأهلية، اربد، الأردن،2016

[2]- الشيخ، خالد ياسين، أمن نظم المعلومات والرقابة (التحكم): ماجستير التأهيل والتخصص في الريادة والإدارة بالإبداع، الهندسة المعلوماتية بجامعة دمشق، 2015، ص21.

– متحكمات الأمن المادي التقنية: وتشمل متحكمات الدخول وكاشفات المقتحمون والإنذارات والمراقبة التلفزيونية والتدفئة والتكييف والطاقة.

– المتحكمات المادية للأمن المادي: مثل الأسيجة والأقفال والإضاءة ومواد البناء والحراس الأمن.

وفيما يخص حماية حقوق الملكية الفكرية للممتلكات الغير مادية يجب تطبيق الحماية على العناصر التالية:

– حماية برامج الحاسوب: تعد برامج الحاسوب أهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف وتوفير الحماية القانونية له، والبرامج المحمية يمكن أن تكون برامج تشغيلية(Windows) أو برامج تطبيقية ((Word/Excel ويمكن أن يكون برنامج عام او تحت الطلب.

– حماية قواعد البيانات: البيانات المخزنة في نظم الحواسيب ليست محل حماية بالنسبة للقوانين والأنظمة، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معينة فإنها تتحول من مجرد بيانات إلى قاعدة معطيات.

– حماية موقع الانترنت: الحماية الفكرية المتعلقة بمواقع الانترنت متعددة، حسب محتوى الموقع والأدوات المرافقة له، فإذا كان المحتوى نتاج عقلي يمكن أن يُحمى بعنوان حقوق المؤلف، وإذا كان الموقع يحوي قاعدة معطيات يُحمى عن طريق حقوقSui Generis التي تحمي قواعد البيانات، اسم المجال يمكن أن يحمى عن طريق حقوق العلامة [1]

3.3 المعايير الدولية لإدارة أمن المعلومات:

ترتكز المعايير الدولية على مجموعة من الإجراءات التي تقترح تطبيقها في مؤسسات المعلومات والاعتماد عليها، وأصدرت منظمة الايزو عدة مواصفات قياسية متخصصة في مجال أمن المعلومات نذكر منها: ISO/MEHARI/ITIL/COBIT وأهم هذه المعايير التي تسمى مواصفات نظم إدارة المعلومات (ISO 27000) وتتكون من ستة معايير فرعية وهي:

– إيزو 27001: يشتمل المعايير الخاصة بالاستمرار على تحسين الخدمات ووضع الأسس اللازمة لضبط ممارسات الأفراد في إدارة أمن المعلومات.

– إيزو 27002: يوفر هدا المعيار المبادئ المعايير الخاصة بتنظيم وإدارة أمن المعلومات.

– إيزو 27003: يوفر هدا المعيار القواعد الخاصة بتنفيذ الإجراءات الإضافية الخاصة بأمن المعلومات.

---

[1]- فيلالي أسماء، شليل عبد اللطيف، مرجع سابق، ص177

– إيزو 27004: يدعم هدا المعيار المقاييس الخاصة بمدى فعالية تطبيق نظم إدارة أمن المعلومات من خلال جملة من الضوابط والمواصفات.

– إيزو 27005: يوفر هدا المعيار مجموعة من المقاييس الخاصة بإدارة المخاطر التي تهدد أمن المعلومات.

– إيزو 27006: يقدم مبادئ وضوابط توجيهية للمنظمات التي تقدم الشهادات الخاصة بالمصادقة على نظام إدارة أمن المعلومات [1].

ومن المعايير الأكثر تطبيقا في إدارة نظم أمن المعلومات وهما (ISO 27001 / ISO 27002) وسوف نتطرق اليها بشيء من التفصيل.

- إيزو 27001: جاءت هده المواصفة الدولية الصادرة عن المنظمة الدولية للتوحيد القياسي بالتعاون مع IEC سنة 2005 وبالاعتماد على المواصفة البريطانية BS7799 التي كانت نتيجة مبادرة مشتركة بين القطاع التجاري والصناعي البريطاني والتي بدأت العمل سنة 1992حيث أصدرت المواصفة البريطانية الأولى BS7799في شباط سنة 1995 حيث مثلت قاعدة ممارسات لإدارة حماية تكنولوجيا المعلومات، ثم استمرت المنظمات بتطوير نظام حماية المعلومات التي أفرزت حل سمي في ذلك الوقت العلاجC الذي تبنى إطار لتطبيق الدعاية الخاصة بحماية المعلومات والتي تم إطلاقها سنة 1997لكن بسبب الصعوبات التي واجهتها عملية تطبيق العلاجC تم تنفيذه عام 2000 ثم مرت المواصفة البريطانيةBS7799 بمراجعة أخرى سنة 2002 وطرأت عليها العديد من التغييرات، ثم بقت كما حتى إصدار المواصفة الدوليةISO27001 في عام 2005 كقاعدة للممارسات والتي تأخذ توجيهاتها وتوصياتها من المواصفة الدولية ISO17799الصادرة سنة 2000 الموازية للمواصفة البريطانية BS7799[2]

يهدف هدا المعيار إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل واستعراض وصيانة وتحسين نظام إدارة أمن المعلومات داخل المنظمات وعادة مات يصلح للتطبيق في مختلف أنواع المنظمات كالحكومية، التجارية ويعتمد على نموذج يعرف بدائرة ديمنج أو نموذج التحسين المستمر للأداء (PDCA: plan-do-

---

[1] – عزة فاروق جهري، طه محمد طه حسن، أمن المعلومات الرقمية وسُبل حمايته في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات، المجلد السادس – العدد الجاني عشر، 2019، ص132.85

[1]– شواو، عبد الباسط. محاضرات غير منشورة في مقياس المعايير والتقييس في الأرشيف. السنة الأولى ماستر تقنيات أرشيفية. جامعة قسنطينة02 عبد الحميد مهري. معهد علم المكتبات والتوثيق. الموسم الجامعي 2015/2014.

check-act) ويتكون من أربعة مراحل متتالية تمثل أحد أهم أليات إدارة الأعمال وتطوير الجودة بالمؤسسات وهي:

مرحلة التخطيط Plan: تأسيس نظام إدارة أمن المعلومات

مرحلة التنفيذ Do: تنفيذ الخطة وتشغيلها

مرحلة التحقق Check: مراجعة النظام بعد تنفيذه وتشغيله

مرحلة العمل Act: صيانة وتحسين أداء وكفاءة النظام

- إيزو 27002: يطلق على هدا المعيار " قواعد ممارسة إدارة أمن المعلومات " وهو أو معيار يصدر عن سلسلة معايير إدارة أمن المعلومات (ISO 27000) الصادرة عن المنظمة الدولية للتوحيد القياسي إيزو، ويهدف هدا المعيار إلى توفير القواعد والمواصفات التي تضبط منهجية إدارة امن المعلومات من خلال الاسترشاد بأفضل الممارسات الأمنية التي من شانها المساعدة في الوصول على الحد الأدنى لأمن المعلومات. حيث صدر سنة 2013 بغية مواكبة التطورات الحاصلة في امن المعلومات وتكنولوجيا الاتصالات فهو يوفر إرشادات حول الممارسات الواجب اتباعها في اختيار وتنفيذ وإدارة أمن المعلومات، وتم اعداده وتصميمه لاستخدامه كمرجع لمعرفة الارشادات والإجراءات الواجب اتباعها لإدارة نظم امن المعلومات إلى جانب المواصفات والخطوات الارشادية الواردة في معيار إيزو 27001 [1].

4. دراسة ميدانية حول أمن الوثائق والمعلومات بالنظام الفرعي لمديرية التربية لولاية قسنطينة:

1.4 التعريف بمكان الدراسة:

1.1.4 لمحة عن مديرية التربية لولاية قسنطينة[2]: هي هيئة إدارية تربوية أنشأت سنة 1889 م مقرها بـ 05 شارع الحرية الكدية قسنطينة، يديرها مدير التربية المعين بمرسوم رئاسي بناء على اقتراح وزير التربية حيث يشرف على إدارة شؤون هذا القطاع الحيوي من هياكل وبناءات ومجمعات مدرسية وتلاميذ وتأطير تربوي وإداري، وهي تعتبر حلقة وصل بين الوزارة الوصية (وزارة التربية الوطنية) ومختلف المؤسسات. يعتبر

[2]– عزة فاروق جهري، طه محمد طه حسن، مرجع سابق، ص119

[2] – وثيقة تعريفية بمديرية التربية من مصلحة الامانة العامة.

مدير التربية آمرا بالصرف، ويتعين عليه إشعار الوالي بالوضعية السائدة في قطاع التربية في الولاية وإفادته بكل المعلومات التي يطلبها منه.

2.1.4 مهام مديرية التربية:

يحددها المرسوم التنفيذي رقم 90-174 المتضمن تنظيم مصالح مديريات التربية ومكاتبها على مستوى الولايات.

يتولى مدير التربية تحت سلطة وزير التربية الوصية:

– إنعاش مجموع النشاطات التربوية في مجال التعليم حسب أطواره الثلاث والتكوين على مستوى قطاع التربية وتنسيقها.

– السهر بالاتصال مع الهياكل والهيئات المعنية على توفير الشروط التي تمكن من الأداء العادي للأنشطة المدرسية والموازية للمدرسة والسير الحسن لمؤسسات التربية والتكوين التابعة للقطاع.

– ويكلف بهذه الصفة في إطار التنظيم الجاري به العمل على الخصوص بما يلي:

– إعداد الخريطة المدرسية لمختلف مراحل التعليم والقيام بتحديثها بالاتصال مع المصالح والهيئات المعنية

– جمع الإحصاءات المدرسية معالجتها، تحليلها والقيام بكل عمليات السير والتحقيقات لتقدير احتياجات الولاية في ميدان التربية.

– السهر على احترام تطبيق المقاييس التربوية في مجال البناءات والتجهيزات المدرسية

– السهر على التنظيم والمتابعة والمراقبة التربوية لمؤسسات التربوية والتكوين الموضوعة تحت وصاية وزير التربية الوطنية.

– القيام بتعيين الموظفين ومتابعتهم وتسيير شؤونهم.

– تنظيم الامتحانات والمسابقات التابعة للقطاع ومتابعتها بالاتصال مع الهياكل والهيئات المؤهلة وتسليم البراءات والشهادات المتعلقة بالامتحانات والمسابقات المذكورة في إطار التنظيم الجاري به العمل.

– تنظيم عمليات التوجيه والتقييم المدرسي.

– تنفيذ عمليات تكوين الموظفين وتحسين مستواهم وتجديد معارفهم.

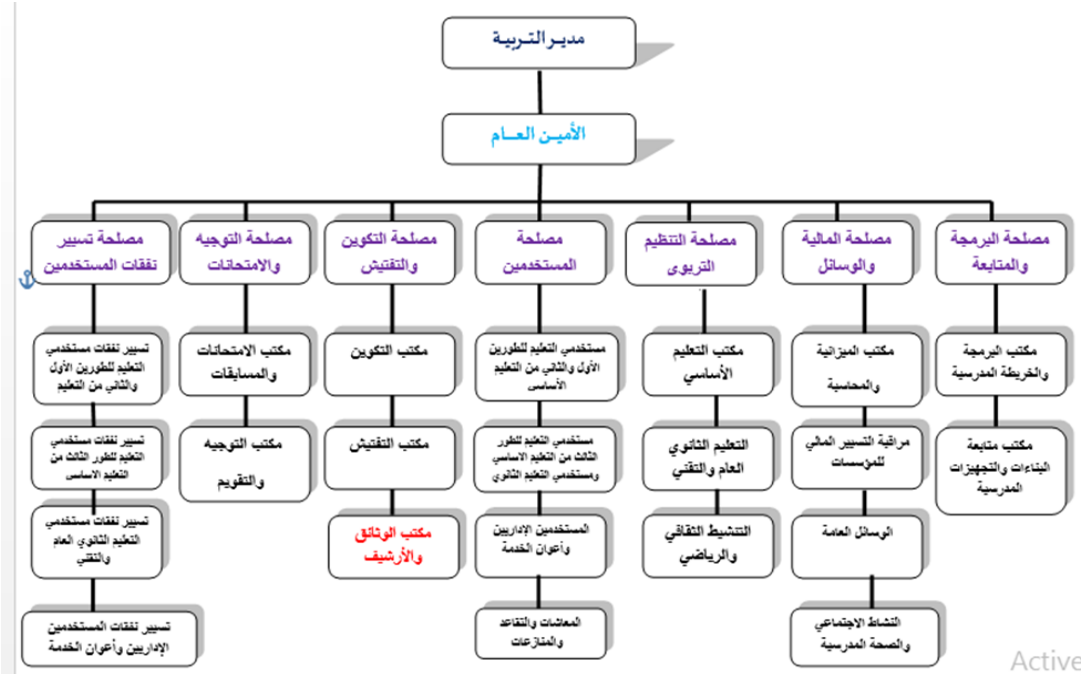
– تنظيم نشاط أسلاك التفتيش وتنفيذه بالاتصال مع المصالح والأجهزة المعنية.

– ترقية الأنشطة التربوية والثقافية في المؤسسات المدرسية، بالاتصال مع القطاعات والأجهزة المعنية.

– السهر على احترام مقاييس حفظ الصحة والأمن في مؤسسات التربية والتكوين التابعة للقطاع

– السهر على تطبيق البرامج والمواقيت الرسمية والتنظيم المدرسي.

3.1.4 مصالح ومكاتب مديرية التربية: تختلف هيكلة مديريات التربية من ولاية لأخرى بحسب المهام المرسومة وعدد المؤسسات التربوية والكثافة السكانية، ومديرية التربية لولاية قسنطينة تتكون من سبعة مصالح رئيسية وهي موضحة في الهيكل التنظيمي التالي:



الشكل رقم 01: الهيكل التنظيمي لمديرية التربية لولاية قسنطينة

من خلال الهيكل التنظيمي أعلاه تبين أن مكتب الأرشيف والوثائق مندرج ضمن مصلحة التكوين والتفتيش، وهو ثالث مكتب للمصلحة بعد مكتب التكوين ومكتب التفتيش، وبالنظر إلى مهام المصلحة والمتعلقة بتكوين الأساتذة والمعلمين الجدد من أجل ادماجهم في محيط العمل أو اقامة دورات تكوينية لتحسين مستواهم، كما تضم المقاطعات التفتيشية عبر الولاية التي تتولى تأطير ومراقبة العملية التعليمية وتوجيهها في المسار الصحيح، أما مكتب الأرشيف الدي يضم وثائق مختلف مصالح مديرية التربية والرزنامة السنوية لتسيير قطاع التربية والمؤسسات التعليمية، والدي كان في وقت غير ببعيد تحت اشراف مصلحة الأمانة العامة للمديرية لكن تم تحويله للمصلحة الحالية بحجة أنه في مديريات التربية الأخرى تابع لمصلحة التكوين والتفتيش.

إن التنظيم الإداري المعمول به والمطبق حاليا يجعل من مكتب الأرشيف مقيدا ومهمشا ومعزولا عن باقي المشاريع الاستراتيجية المنجزة سواء داخل المؤسسة أو خارجها، وهدا الإشكال ليس حكرا على مكتب أرشيف مديرية التربية فقط وإنما العديد من مصالح الأرشيف المتواجدة بمختلف المؤسسات تعاني من نفس المشكل. مما

يستدعي من الجهات المعنية بإصدار قوانين الأرشيف كالمديرية العامة للأرشيف ومؤسسة الأرشيف الوطني إلى التنسيق مع كل الوزارات والمؤسسات لإعادة النظر في تنظيم مصالح الأرشيف في الهياكل التنظيمية للمؤسسات وإصدار قوانين وتعليمات مشتركة من شأنها اعادة تحيين التنظيمات الإدارية السابقة وتكييفها لمجابهة التحديات الحديثة حتى تستجيب لمتطلبات مشاريع التنمية، ومنه فسح المجال أمام الأرشيفي الدي طالما تم تهميشه في الإدارات وأصبح دوره يقتصر على حماية مخازن الوثائق البالية لا غير.

انطلاقا من المقابلة التي اجريناها مع مدير مشروع الرقمنة تم جمع البيانات وتبويبها على النحو التالي:

1.5 مصطلحات عامة حول أمن المعلومات:

في البداية ارتأينا أن نستهل مقابلتنا التي اجريناها مع مدير مشروع الرقمنة بوضع مجموعة من المصطلحات ذات العلاقة بموضوع دراستنا وترتبط به ارتباطا وثيقا بغرض معرفة مفهومها من طرف مدير المشروع وكأداة تمهيدية لمعرفة مدى إحاطته بموضوع أمن المعلومات والوثائق الإلكترونية، حيث كانت بدايتنا بمصطلح أمن المعلومات حيث أبرز مدى وعيه بأهمية هدا المصطلح والمكانة الكبيرة التي يحتلها ضمن أنشطة ووثائق المؤسسة، حيث اعتبره بأنه توفير الحماية للبيانات الرقمية من سوء استخدامها خارج نطاقها، ومن خلال هدا التعريف نجد أنه يفتقد إلى بعض العناصر الضرورية والمؤثرة في المصطلح ودلالته، لأن الماهية العامة لأمن المعلومات تشمل مختلف السياسات والأدوات والاستراتيجيات المعتمدة لمنع وكشف وتوثيق وصد مواجهة التهديدات على المعلومات سواء كانت رقمية أو غير رقمية. ثم انتقلنا إلى المصطلح الثاني المتمثل في الاعتداء الإلكتروني والاختراق الدي في جمع فيه مدير المشروع بين المصطلحين وخصهما بمفهوم واحد فكانت إجابته أن " الاعتداء الالكتروني هو اختراق الحماية الالكترونية وسلب البيانات وتعطيل عمل الرقمنة" وهدا التعريف لم يقدم مفهوما سليما وشاملا للاعتداء الالكتروني الدي يتمثل في كونه دلك السلوك العدواني المتعمد الدي يستخدم الوسائط الالكترونية من أجل التحرش – المضايقة – من احراج، تخويف، وتهديد الأخرين. أما المصلح الثاني المتمثل في الاختراق فيتمثل في القدرة على الوصول إلى هدف معين بطرق غير مشروعة من خلال ثغرات في نظام الحماية الخاص بالهدف. أما المصطلح الثالث المتمثل في الثغرة الأمنية لم يتمكن مدير مشروع الرقمنة من اعطائنا تعريف واضحا حول هدا المصطلح والدي يقصد به تلك المناطق الضعيفة في أنظمة تشغيل الحواسيب، هده المناطق يمكن التسلل عبرها إلى داخل النظام ومن ثم يتم التعديل فيه وقد يصل الحد إلى تدميره نهائيا، ومنهم من يسميها الثغرة التقنية التي تعتبر نقطة ضعف ما في نظام معين تتيح للمخترقين التسلل من خلالها لتدمير نظام معين أو سرقته. وبالانتقال إلى مصطلح الاحتيال

الالكتروني والقرصنة الدي لا يقل أهمية عن المصطلحات السابقة فقد اعتبر مدير المشروع أنهما تسمية لمصطلح واحد أي أن " الاحتيال الإلكتروني هو القرصنة" وهدا مخالف لما هو متعارف عليه لأن الاحتيال الالكتروني يقصد به التصيد الاحتيالي ويستخدمه مجرمو المعلومات لاستدراج مستخدم شبكة الأنترنيت للكشف عن معلومات شخصية بغرض استخدامها لصالحهم، بيد ان القرصنة هي اقتحام نظام الكمبيوتر لسرقة المعلومات السرية الخاصة باستخدام حيل وطرق ملتوية.

وفيما يتعلق بصيغتي التوقيع والتصديق الالكترونيين فقد صدر القانون الجزائري[1] رقم 15-04 في الجريدة الرسمية الجزائرية مند فيفري 2015 ولكن لم يتم تطبيقه بعد لعدم صدور النصوص التنظيمية التي تفسر طرق وكيفيات تفعيله بمختلف الإدارات، حيث افادنا مدير المشروع بأنه عند تطبيق القانون فإنه لم نعد بحاجة إلى الإمضاء والمصادقة الورقية كما في السابق حيث نلاحظ أن هدا التعريف سطحي يفتقد إلى الشرح والتفسير لأن التوقيع الإلكتروني عبارة عن ملف رقمي (شهادة رقمية) تصدر عن أحد الهيئات المتخصصة والمستقلة ومعترف بها من الحكومة تماما مثل كتابة العدل وفي هذه الملف يتم تخزين اسمك وبعض المعلومات المهمة الأخرى مثل رقم التسلسل وتاريخ انتهاء الشهادة ومصدرها، وهي تحتوي عند تسليمها لك على مفتاحين (المفتاح العام والمفتاح الخاص) ويعتبر المفتاح الخاص هو توقيعك الإلكتروني الذي يميزك عن بقية الناس أما المفتاح العام فيتم نشرة في الدليل وهو متاح للعامة من الناس. أما التصديق الإلكتروني فهو عملية تضمن أربعة (04) جوانب أمنية لتبادل المعلومات على شبكة الإنترنت وهي: السرية والتوثيق والنزاهة وعدم الاستنكار. كون هذه الجوانب تسمح في إرساء مناخ ثقة عن طريق إقامة بنية ذات مفتاح عموميpublic key infrastructure «PKI» بنية ذات مفتاح عمومي تساعد البنية ذات المفتاح العمومي على تحديد أصحاب المفاتيح عن طريق إصدار شهادات إلكترونية. وختمنا مجموعة المصطلحات ومفاهيمها بمصطلحي الأرشفة الإلكترونية والحفظ الرقمي اللدان يعتبران أساسيان في البيئة الرقمية، حيث أجاب قائد المشروع بأن الحفظ الرقمي هو " حفظ البيانات لضمان استرجاعها عندما تستدعي الحاجة " وعند التمعن في التعريف نجد أنه سطحي لا يغوص في المفهوم الحقيقي للحفظ الرقمي بأبعاده العلمية والعملية حيث ان الحفظ الرقمي هو سلسلة من الإجراءات اللازمة لضمان استمرار إمكانية الوصول إلى

[1] – القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، متاح عبر http://www.joradp.dz/fta/jo-arabe/2015/a2015006.pdf تاريخ الزيارة: 2020/04/05.

المواد الرقمية كلما كان ذلك ضروريا فهو يجمع بين السياسات والاستراتيجيات والإجراءات لضمان الوصول وتهيئة وتوليد محتوى رقمي بغض النظر عن التحديات التي تواجه فشل الوسائط والتغير التكنولوجي. هدف الحفظ الرقمي هو استخلاص دقيق لمحتوى موثوق على مر الزمن.

2.5 فكرة مشروع الأرضية الرقمية والجدوى منها: يعتبر مشروع الأرضية الرقمية لقطاع التربية الوطنية من المشاريع الرائدة ضمن سياسة الجزائر الإلكترونية حيث قامت بتنفيذه وزارة التربية الوطنية بعد التخطيط له مسبقا ومر بعدة مراحل: [1]

– بدأت الفكرة منذ سنة 2010 إذ قامت وزارة التربية الوطنية بدراسة حول اختيار البرمجيات التي تناسب تسيير القطاع عبر مديريات التربية الـ 50 على مستوى الوطن.

– وفي سنة 2015 تم تنظيم ملتقى وطني بوزارة التربية الوطنية حضره كافة مديري التربية ورؤساء المصالح وإطارات في الإعلام الآلي حضرته ممثلة عن شركة Microsoft وممثل عن شركة تركية من أجل عرض منتجات شركتهم، لكن لم يتم الاتفاق مع الشركتين السابقتين.

– وفي السنة نفسها (2015) قامت مديرية التربية لولاية سطيف بتقديم اقتراح (قاعدة بيانات) لتسيير ملفات المستخدمين، ومديرية التربية لولاية الوادي قاعدة بيانات لتسيير التلاميذ، ومديرية التربية لولاية ورقلة قاعدة بيانات لتسيير مختلف الهياكل والمؤسسات التربوية. وتم تشكيل خلية إعلام آلي بوزارة التربية من أجل إنشاء البرمجية الحالية المستخدمة التي تعمل عبر الويب.

حيث كانت بوادر إطلاق المشروع خلال الندوة الوطنية المنعقدة في ثانوية الرياضيات بالقبة الجزائر العاصمة يومي 26 و27 مارس2015، وتم وضع برنامج عمل لسير المشروع، ونُصبت لجنتين تتكفل الأولى بقيادة مشروع الرقمنة، واللجنة الثانية المتكونة من مهندسين وتقنيين مسؤولين عن تنفيذ البرنامج على مستوى مديريات التربية على مستوى كل الولايات، وقد مر المشروع بمرحلتين:

المرحلة الأولى: تصميم وإنجاز تطبيق ويب من قبل الفرق التقنية، وهذا بعد عدة لقاءات وبحضور خبراء ومستشارين.

المرحلة الثانية: بعد إجراء عدة اختبارات ناجحة على هذا التطبيق الجديد انطلقت عملية إدخال البيانات إلى نظام المعلومات عبر كافة مديريات التربية الولائية على مستوى الوطن. ونظرا لحجم القطاع وأهميته من

[1] – مقابلة مع مدير مشروع الرقمنة بتاريخ:2019/12/22 بمكتبه مديرية التربية لولاية قسنطينة

حيث عدد التلاميذ وعدد المستخدمين والمؤسسات التربوية، إذ يضم قطاع التربية على مستوى الوطن 09 ملايين تلميذ، 000 700 مستخدم (ة)، و000 27 مؤسسة تعليمية [1]، فقد تم تقسيم مشروع رقمنة قطاع التربية إلى ثلاثة أنظمة فرعية:

- مشروع تسيير تمدرس التلاميذ.
- مشروع تسيير المؤسسات التربوية (الهياكل)والسكنات الوظيفية.
- مشروع تسيير المستخدمين.

والجدوى من مشروع الأرضية الرقمية هو سعي وزارة التربية الوطنية إلى تذليل كافة الصعوبات التي كانت تعاني منها في الحصول على مختلف المعلومات من مديريات التربية عبر الوطن وحسب ما جاء به المنشور 89 المؤرخ في 21 جوان 2015 فإن المشروع يهدف إلى:

- توحيد مختلف الوثائق الخاصة بتسيير مناصب المستخدمين
- وضع ترميز وطني لمختلف رتب المستخدمين من أجل الاستغلال الأمثل لها
- ربح الوقت وتخفيف النفقات في إطار معالجة ملفات المستخدمين وتخفيف الأخطاء أو القضاء عليها نهائيا
- جعل تسيير مصلحة المستخدمين أكثر جلاء ووضوح.

ومن خلال الأهداف أعلاه يتبادر إلى ذهننا تساؤل بخصوص ادا ما تم تسطير سياسات وخطط لتوفير الأمن والحماية للمعلومات والوثائق الإلكترونية التي تخص القطاع وبالتالي تسليم الدور للأرشيفي الدي يشرف على والعناية بالأرشيف وضمان ديمومته وحفظ الأرشيف على المدى الطويل وهدا ما سنتطرق اليه في العنصر الموالي.

3.5 دور الأرشيفي في مشروع الأرضية الرقمية: اتضح عدم اشراك الأرشيفي في المشروع ولم يأخذ بأفكاره وأراءه ونصائحه، ونفس الشيء يحدث في مختلف مشاريع الرقمنة في المؤسسات الأخرى، حيث يهمش الأرشيفي دائما ولا يستشار ويغيب دوره لسبب او لأخر... ولأنهم يجهلون الدور الأساسي والفعال الذي يقوم به فانهم لا يعيرونه أي اهتمام، وأكبر دليل على هدا القول في السؤال الموالي حول كيفية تعاملهم مع معيار ISO 15489 فكانت الإجابة بالسلب وانهم لا يعرفون هدا المعيار اطلاقا؟ وهده هي الفجوة

[1]- نشرة احصائية بمكتب الإحصاء بمديرية التربية لولاية قسنطينة للموسم الدراسي 2020/2019 .

الكبيرة التي لا يملأها الا الأرشيفي دون غيره، خاصة للأهمية الكبيرة التي يلعبها هدا المعيار في تسيير الأرشيف الجاري والوسيط في البيئتين، ولأنهم تجاهلون هدا المعيار فان تسيير الوثائق يكتنفه الخلل والغموض وتكون النتائج وخيمة مستقبلا، حيث أنه صدر هذا المعيار (معيار ISO 15489) [1] سنة 2001 عن اللجنة الفنية ISO/TC 46 المعلومات والتوثيق: تسيير الأرشيف الإداري وهو عبارة عن دليل لتنظيم وتسيير المعلومات والوثائق المنتجة أو المستلمة من طرف أي مؤسسة عمومية أو خاصة، في إطار القيام بنشاطاتها، حسب مهام وأهداف هذه المؤسسة. يساعد في تحديد مسؤوليات المؤسسات اتجاه الأرشيف الجاري أو الوثائق بشكل عام، مهما كان شكلها أو ووعائها، يساعد كذلك في تحديد سياسات وطرق تحمل هذه المسؤوليات. صمم كداعم لصيرورة نوعية، بالتطابق مع المعيارين ISO14001 الخاص بالمحيط، و ISO 9001 الخاص بمراقبة النوعية، يعد كدليل لتصميم نظام أرشفة ووضعه في حيز التنفيذ. وهو يشمل على جزئين:

الجزء الأول: المبادئ الرئيسية

الجزء الثاني: الدليل التطبيقي (التقرير التقني)

حيث يضمن المعيار:

- وضع السياسات والمعايير.
- تقييم المسؤوليات والمعايير.
- إعداد الإجراءات والنصوص القانونية الموافقة عليها ونشرها.
- تصميم الأنظمة الخاصة بتنظيم وتسيير الوثائق الأرشيفية ووضعها حيز التنفيذ وصيانتها.
- إدماج تسيير الأرشيف الإداري في الأنماط التنظيمية وأساليب العمل.

ولو ان أغلب الهيئات والمؤسسات الأرشيفية بادرت باستخدام وتطبيق مثل هده المعايير والمواصفات في تسيير وإدارة وتخزين وثائقها في البيئتين التقليدية والرقمية لتغلبت عن الكثير من المشاكل والمعوقات في التسيير المستقبلي والإتاحة لهده الوثائق سواء داخليا عبر الشبكة المحلية أو عبر شبكة الأنترنيت.

---

[1]- بشير، عماد: مسار الوثائق الإدارية و معالجتها، كلية الإعلام و التوثيق، الجامعة اللبنانية، متاح على الخط: http://www.al-raeed.net/training تاريخ الزيارة (2020/05/24)

وما يعاب على القائمين على مشروع الأرضية الرقمية –فرع مديرية التربية لولاية قسنطينة – أنهم عند توظيف الطاقات التقنية للمشروع فقد اكتفوا بتوظيف مهندسين في الاعلام الالي من قطاع التربية فقط دون الاستعانة بخبرات من خارجه وحتى من خارج الوطن لان مثل هده الخبرات أغلبها سبق وان ساهم في مشاريع رقمية مماثلة وتراكمت لديه مجموعة من المهارات والقدرات مما يضفي لمسة وإضافة مفيدة للمشروع.

وفيما يخص الخدمات الإلكترونية والوثائق التي تتيحها الأرضية الرقمية عبر نظامها المعلوماتي فإنها تنقسم إلى ثلاثة فروع كبيرة حسب هيكل الأرضية الرقمية وأقسامها الثلاثة (نظام تسيير المستخدمين، نظام تسيير تمدرس التلاميذ، نظام تسيير الهياكل والسكنات الوظيفية)، وسوف نوردها بالتفصيل [1]

اسم النظام	طبيعة الخدمات/الوثائق	نوع الإتاحة
نظام تسيير المستخدمين	– محضر التنصيب، مجمل الخدمات، مقرر التعيين، شهادة عمل – رخصة الدخول المؤقتة، رخصة الخروج المؤقتة – التأهيل المرغوب فيه، جداول ترتيب المترشحين المسجلين في قوائم التأهيل – جدول الترقية في الدرجة والقرار – القائمة الإسمية للموظفين – حصية استغلال القوائم الاحتياطية – الملف الإلكتروني للموظف – الغيابات الشهرية للموظفين – استدعاء المترشحين في القوائم الاحتياطية – وصل استلام التعيين الخاص بالمترشحين في القوائم الاحتياطية – منحة المردودية والأداء التسييري	عبر المؤسسة التي ينتمي اليها المستخدم
	– استمارات معلومات التلميذ – الملف الإلكتروني للتلميذ – شهادة التسجيل/شهادة مدرسية – اشعار بعدم الالتحاق (التسجيل)	

[1]– وزارة التربية الوطنية، منشور رقم: 2018/230 الإطار المرجعي المتعلق بالنظام المعلوماتي لقطاع التربية الوطنية.

نظام تسيير تمدرس التلاميذ	– اشعار بالغياب/الاعذار/قرار الشطب – طلب تحويل التلميذ/ شهادة تغيير المؤسسة – كشف نتائج تقويم الفصل – بطاقة الرغبات/ بطاقة المتابعة والتوجيه	عبر المؤسسة التي ينتمي اليها المستخدم
نظام تسيير الهياكل والسكنات الوظيفية	– البطاقة الوصفية للمؤسسة – قائمة المؤسسات حسب البلدية – الدليل الولائي للمؤسسات / الدليل الوطني للمؤسسات – الحصيلة الولائية لهياكل المؤسسات/ الحصيلة الوطنية لهياكل المؤسسات – مقرر منح السكن الوظيفي لضرورة الخدمة الملحة/ مقرر الإلغاء لنفس الصيغة – مقرر منح السكن الوظيفي لمنفعة الخدمة / مقرر الإلغاء لنفس الصيغة – وضعية السكنات – شهادة تبرئة الذمة الخاصة بالسكن الوظيفي – أمر بإخلاء السكن	في خلية الرقمنة بمديرية التربية

الجدول رقم (03) يمثل مخرجات النظام المعلوماتي لقطاع التربية

من خلال الجدول أعلاه يتضح ان الوثائق التسييرية بقطاع التربية الوطنية تم تجهيزها واعدادها بغرض توحيد مخرجات النظام المعلوماتي وتكامله ليشمل المهام وبالتالي توحيد الإجراءات والعمليات عبر المديريات الولائية للتربية البالغ عددهم 50 مديرية عبر الوطن. ومنه ربح الوقت والجهد واختزال المسافات والسعي لتحقيق مبدا الجودة.

ويبقى دائما أكبر نقص تعاني منه الوثائق الإلكترونية هو الحجية القانونية بسبب عدم تطبيق ألية التوقيع والتصديق الإلكترونيين برغم صدور القانون في الجريدة الرسمية الجزائرية مند فيفري 2015 لكن يبقى حبر على ورق والسبب في ذلك هو عدم سن وتشريع القوانين التنظيمية التي تبين طرق وكيفيات تطبيقه واعتماده في المؤسسات بمختلف أنواعها، وفي قطاع التربية نفس الشيء فالوثائق الإلكترونية الناتجة عن مشروع الرقمنة تبقى رهينة التوقيع اليدوي التقليدي ويجب المصادقة عليها وإمضائها من طرف مدير المؤسسة التي تنتمي إليها.

وفي سؤالنا حول طريقة حماية وسائط التخزين الداخلية والخارجية كانت إجابة مسؤول الرقمنة بمديرية التربية [1] أن هدا الأمر يتم على مستوى النظام المركزي بوزارة التربية الوطنية وليس لديه معلومات كافية بخصوص هده النقطة، أما على مستوى مديرية التربية قسنطينة فلا توجد وسائط تخزين خارجية وأن كل البيانات موجودة بالنظام الفرعي للمديرية الموصول بالنظام الأساسي على مستوى الوزارة الوصية، ومن هنا نستنتج أن منظومة الحفظ هشة ولا توجد استراتيجية حفظ خاصة بالوثائق والمعلومات تستند إلى المعايير والمواصفات العالمية الجاري بها العمل.

4.5 تقييد البيانات بالأرضية الرقمية وسبل حمايتها: في المحور المتعلق بتقييد البيانات بالنظام المعلوماتي للأرضية الرقمية وسبل حمايتها وتأمينها من مختلف المخاطر التي تتربص بها ومصادرها تناولنا عدة عناصر لفحص الظاهرة واستنباط واقعها، نبدأ بالموارد البشرية العاملة في مشروع الرقمنة بمختلف رتبهم ومؤهلاتهم العلمية والتقنية وهي كما يلي:

نوع المنصب	المؤهل	الخبرة	د. تدريبية	العدد
رئيس مكتب	شهادة ليسانس علوم قانونية	05 سنوات	01	01
مهندس دولة في الإعلام الآلي	شهادة مهندس دولة في إ. الآلي	من 05 إلى 12 سنة	/	05
متصرف إداري	شهادة ليسانس علوم قانونية	من 05 إلى 11 سنة	/	02
تقني سامي في الإعلام الآلي	شهادة تقني سامي في إ. الآلي	من 05 إلى 15 سنة	01	07
عون إدارة	مستوى ثانوي + تخصص إداري	من 06 إلى 10 س	01	02
كاتب مديرية	مستوى ثانوي + شهادة سكر	من 05 إلى 15 سنة	01	02

الجدول (04): يمثل الموارد البشرية العاملة في مشروع الرقمنة

[1] – مقابلة مع مدير مشروع الرقمنة بتاريخ:2019/12/22 بمكتبه مديرية التربية لولاية قسنطينة

نلاحظ من خلال الجدول أعلاه أن العدد الأكبر من أفراد مشروع الرقمنة يتمثل في رتبة التقنيين السامين في الإعلام الآلي الذي بلغ عددهم 07 أفراد، تليهم رتبة مهندس دولة في الإعلام الآلي بـ 05 أفراد، وذلك لأن حاملي هذه الرتب هم مسيرين إداريين في مصلحة المستخدمين وعلى دراية تامة بكل العمليات التي تخص ملف المستخدم، إضافة إلى تحكمهم في تطبيقات الحاسوب ولهذا تم توظيفهم في مشروع الرقمنة للاستفادة من خبرتهم وكفاءتهم، في حين نلاحظ تذبذب عدد الأفراد الأخرى ويرجع ذلك لقيامهم بوظائف ثانوية في مشروع الرقمنة كتجميع استمارات المستخدمين والتحقق من المعلومات المدونة بها، ما عدا رئيس المكتب الذي تمكن وظيفته في الإشراف على المسيرين التابعين لمكتبه.

أما النقص الملاحظ يكمن في الغياب التام للأرشيفي أو الذي لم يتم إشراكه في تنفيذ مشروع الرقمنة، ويمكننا تبرير ذلك بالفكرة السلبية السائدة في مختلف المؤسسات والإدارات مفادها أن الأرشيفي يقتصر دوره في المحافظة على الوثائق القديمة فقط، ويجهلون الدور الفعال الذي بإمكانه تأديته في مشروع الرقمنة، واستفادتهم من مؤهلاته وخبراته التي اكتسبها خلال مساره الجامعي فيما يخص تنفيذ مشروع الرقمنة.

ننتقل الأن الى **الضوابط المستخدمة في حماية وأمن الوثائق والمعلومات** فإن مدير مشروع الرقمنة أفادنا بأن عملية دخول المستخدم إلى ملفه الإلكتروني يكون عن طريق اسم المستخدم وكلمة المرور بمؤسسة عمله (بالنسبة للمستخدمين) والتلاميذ بالمؤسسة التي يدرس وتحت تصرف المؤسسة دائما. حيث قامت وزارة التربية الوطنية في هدا الصدد بأخذ التدابير اللازمة من أجل حماية النظام الآلي من الأخطار التي تهدده، ويبرز دلك من خلال وضعها لجملة من التوصيات عبر ثلاثة محاور كبرى وهي [1]

أ. **سرية الحسابات الإلكترونية**: باعتبار الحساب الإلكتروني الهوية الرقمية التي تسمح للمستخدم بالولوج إلى خدمات النظام المعلوماتي في حدود المهام الموكلة إليه وجب اتخاذ التدابير اللازمة لحمايتها والحفاظ على سريتها باعتبار كلمات المرور خط الدفاع الأول في مواجهة الاختراق والدخول غير المرخص والقرصنة والجرائم الإلكترونية والتخريب، لذلك يجب:

- اختيار كلمات مرور معقدة
- يتم تغييرها بانتظام

[1] - منشور رقم: 2018/230 الإطار المرجعي المتعلق بالنظام المعلوماتي لقطاع التربية الوطنية.

– الحرص على عدم التصريح بها
– لا ينبغي تقاسمها أو تخزينها داخل ملف أو على الورق من دون حماية ملائمة
– عدم استخدامها خارج إطارها الرسمي المسموح به (ميثاق أمن المعلومات)
– عدم استخدام البرامج المساعدة التي يتم نشرها عبر الأنترنيت من طرف مطوريها لاستدراج ضحاياهم للحصول على المعلومات المتعلقة بالحساب لتسهيل تنفيذ الهجمات الإلكترونية

ب. حماية البيانات والمعلومات: وبخصوص الحرص على سرية البيانات والمعلومات الشخصية فإن كل مستخدم يمتلك حسابا في النظام المعلوماتي عليه أخذ كافة الإجراءات الضرورية لضمان سرية المعلومات والبيانات التي اطلع عليها في إطار تأدية مهامه ولا يجوز له إفشاء أو تحويل أو إعلان أو نشر تلك المعلومات لأي غرض كان، كما يمنع تداولها في فضاءات خارج الفضاء الإداري الرسمي المخصص لهدا الغرض.

ت. تغيير المستخدم المكلف بتحيين المعلومات: وفي هده الحالة إدا تم تغيير المستخدم المكلف بتحيين المعلومات والبيانات يلزم ذات المستخدم بتسليم المعلومات الخاصة بالحساب الإلكتروني (اسم المستخدم وكلمة المرور) والتي يجب تغييرها فورا بعد عملية التأكد من صحتها من طرف خليفته، ويبقى المستخدم المعفى من العملية مسؤولا شخصيا واخلاقيا وجزائيا على المعلومات التي أطلع عليها في إطار مهمته المنتهية.

وفيما يتعلق بالوسائل المستخدمة في التصدي والوقاية من هده الاخطار فيستخدمون جدار النار ومضاد الفيروسات حيال ذلك، ومن المناشير الداعية للوقاية من المخاطر المتعددة المنشور رقم 1098 بتاريخ: 25 ماي 2017. ف/ي التدابير الوقائية ضد الهجومات الالكترونية (بخصوص فيروس Ransomware)

كما أفادنا مدير مشروع الرقمنة بالمديرية أن **وتيرة تحيين البيانات المحتواة في النظام الفرعي تكون يومية** يقوم بها المكلفين بتقييد البيانات بالنظام بمختلف أصنافهم والدين يشرفون على تسيير المصالح والمكاتب الإدارية بمديرية التربية لولاية قسنطينة تحت إشرافه دائما، وتقتضي عملية التحيين إضافة التعديلات الجديدة التي تطرأ على البيانات المقيدة بالنظام، نأخذ على سبيل المثال لا الحصر المعلومات الشخصية للمستخدمين التي تطرأ عليها تغييرات مثل ترقيته، تحويله، تقاعده...الخ

وفي **عملية التحقق من سلامة البيانات** من أي تحريف أو تغيير مقصود أو غير مقصود أفادنا مدير المشروع بأن البيانات المقيدة بالنظام الفرعي مسؤول على سلامتها وأمنها أصحاب المفاتيح عبر مختلف المكاتب والمصالح بالمديرية وهم يتحملون المسؤولية الكاملة من أي تزوير أو تعديل غير قانوني، أما فيما يخص

الأخطاء الغير مقصودة عند تقييد البيانات فعادة ما ينتبه إليها المستخدمين الى الأخطاء عند استخراج وثائقهم حيث يتم ابلاغ مؤسستهم التربوية عند دلك والمتمثلة في مدير المؤسسة الدي بدوره يقوم ارسال البيانات إلى الجهة المكلفة بالتصحيح على مستوى مديرية التربية.

وفي هدا الصدد دائما وعند سؤالنا حول إدا ما توجد أليات يتم من خلالها التحقق من الوصول إدا كان وصول مشروع أو غير مشروع فكانت الإجابة سلبية وأنه لا تتوفر أي وسيلة يتم من خلال تأمين الوصول للبيانات والمعلومات بالنظام الفرعي وكشف المحتالين وردعهم، وهده يمكن اعتبارها فجوة أمنية لتسريب والعبث بالمعلومات الشخصية للمستخدمين أو للتلاميذ ونفس الحال بالنسبة لمعلومات إدارية أخرى، لأن المنتحل يتحصل على كلمة السر واسم المستخدم بأحد الطرق الملتوية ويستطيع الولوج الى الملف الإلكتروني للمستخدم والحصول على معلومات حول حياته الشخصية أو المهنية شأنه شأن صاحب الحساب، ومن ثم يطبعها وينسخها ويستخدمها لأغراض لا مشروعه ولا يتم كشفه أو التوصل إلى هويته المزيفة لعدم وجود شفرات ومفاتيح خاصة تخص صاحب الحساب دون غيره. وبالرغم أن الحماية تتم على ثلاثة مستويات (حماية النفاذ، حماية القواعد والحماية من الفيروسات) لكن حماية الوصول تبقى النقطة المهمة التي وجب اعطائها أكبر قدر من التأمين والتشفير.

6. نتائج الدراسة: خلصت دراستنا إلى مجموعة من النتائج أبرزها:

– مشروع رقمنة قطاع التربية إلى ثلاثة أنظمة فرعية وهي (نظام تسيير تمدرس التلاميذ، نظام تسيير المؤسسات التربوية الهياكل والسكنات الوظيفية ونظام تسيير المستخدمين)

– يهدف مشروع الأرضية الرقمية لتحقيق ما يلي:

توحيد مختلف الوثائق الخاصة بتسيير مناصب المستخدمين

وضع ترميز وطني لمختلف رتب المستخدمين من أجل الاستغلال الأمثل لها

ربح الوقت وتخفيف النفقات في إطار معالجة ملفات المستخدمين وتخفيف الأخطاء أو القضاء عليها نهائيا تحقيق الشفافية في التسيير.

– لم يتم اشراك الأرشيفي في المشروع ولم يأخذ بأفكاره وأراءه ونصائحه عند تنفيذ مشروع الأرضية الرقمية أو في وضع خطط حماية وأمن الوثائق والمعلومات.

– انعدام تطبيق المعايير والمواصفات العالمية للمعلومات مثل معيار ISO 15489 (الخاص بتسيير الأرشيف الجاري والوسيط) وكدا المعايير الدولية لأمن المعلومات مثل معيار ISO 27000 وفروعه الستة.

– اكتفى القائمون عن مشروع الأرضية الرقمية بتوظيف طاقات بشرية من داخل القطاع فقط دون الاستعانة بخبرات خارجية التي كان بإمكانها تحقيق إضافة للمشروع سواء في اقتراح ووضع خطط واستراتيجيات لتامين وحماية المعلومات أو في مشروع الرقمنة بصفة عامة.

7. مقترحات الدراسة:

بناءا على النتائج التي توصلنا إليها من خلال دراستنا نقترح ما يلي:

– ضرورة اشراك ودعم اسهام كل الأطراف الفاعلة عند إقرار وتصميم ووضع الاستراتيجية الأمنية لقطاع التربية الوطنية بما فيها الأرشيفيين والمختصين في امن المعلومات من داخل وخارج القطاع. والمراجعة الدورية لها لمعرفة النقائص واستدراكها في الوقت المناسب.

– اليقظة الاستراتيجية والعمل على مسايرة المستجدات الحاصلة في مجال أمن المعلومات والتعرف على الطرق المستحدثة في الاختراق والسطو على المعلومات والطرق والتقنيات الحديثة لمحاربتها.

– إعداد دورات تكوينية للعاملين في النظام الفرعي لمديرية التربية أو على مستوى الوزارة الوصية عن طريق بغية تطوير مهاراتهم وقدراتهم وتأهيلهم لمسايرة أخر المستجدات في المجال.

– تحسيس وتوعية المنتمين لقطاع التربية بضرورة حماية بياناتهم الشخصية والسرية في استخدام كلمات المرور وتغييرها بشكل دوري حتى لا يقعوا في كمين الاختراق.

– اعتماد وتطبيق المعايير والمواصفات الدولية الخاصة بإدارة وتسيير الوثائق الالكترونية في البيئة الرقمية أو تلك المتعلقة بأمن نظم المعلومات.

– ضرورة تطبيق صيغتي التوقيع والتصديق الالكترونيين لما توفر من فوائد ومنافع سواء بالنسبة لحجية الوثيقة الالكترونية أو لتجنب التزوير والتحريف للمعلومات.

– استخدام استراتيجيات الحفظ الرقمي بالأرضية الرقمية (التهجير، المحاكاة، النسخ الاحتياطي) لضمان تأمين المعلومات من الاخطار الفجائية.

– سن قوانين وتشريعات موحدة على المستوى الوطني والعربي لحماية وأمن المعلومات في البيئة الرقمية ومعاقبة الفاعلين أو المتسببين في المساس بأمن المعلومات.

8. خاتمـــــة:

في الختام يمكن القول إن المعلومات هي المورد الأهم بالمؤسسة التي لا تزول بزوال الأفراد لأنها تضم ذاكرتها وتوثق لحاضرها وتخطط لمستقبلها، وحت تتم كل هده الأنشطة على أحسن وجه وجب توفير الرعاية والعناية بالمعلومات وضرورة تأمينها خاصة في العصر الرقمي الدي نعيشه أين أصبحت حلقة الحفظ

واسترجاع البيانات والمعلومات هي أضعف حلقة في السلسلة الوثائقية بسبب المؤثرات الخارجية أولها الشبكة العنكبوتية وما أفرزته من مخاطر مباشرة وغير مباشرة مما يخلف قرصنة وتحريف المعلومات والتلاعب بمحتواها، ثانيا هشاشة وسائط التخزين ومحدودية عمرها مما يتسبب في ضياع المعلومات وفقدانها، وثالثا إهمال المؤسسة لعنصر أمن المعلومات وعدم وضع الخطط والأدوات المتاحة لحماية المعلومات والعمل على إطالة عمرها، رابعا ضعف البنى التحتية لتكنولوجيا المعلومات ونقص الكادر البشري المؤهل وعدم تمكنه من التحكم في أخر التقنيات الحديثة ومسايرتها. كل هده النقائص تعاني منها دول العالم الثالث بشكل عام والدول العربية على وجه الخصوص لكن الأمر يختلف في الدول الغربية التي تتوفر على كل المقومات والدعامات التي تساعد في حماية المعلومات وتطبيق سياسة أمن محكمة لحفظها على المدى البعيد.

ولأن مصطلح أمن المعلومات يشير إلى نظام متكامل يضم مجموعة من التدابير والإجراءات والوسائل يسيرها العنصر البشري باعتباره مورد أساسي في أي منظمة والدي يمكن أن يؤدي دورا إيجابيا في النظام إدا ما تم استثماره بشكل أفضل وتنمية خبراته ومهاراته في مجال حماية وتأمين الكيانات الرقمية، كما يمكن أن يحدث ثغرة وخطرا على المنظومة بأكملها. ولهدا وجب إعطاء الأهمية والأولوية للمورد البشري وحسن اعداده وتكوينه على استخدام الوسائل والمعدات والتقنيات الأمنية ومسايرة أخر المستجدات في الميدان أيضا طريق اشراكه في التربصات الوطنية أو الدولية وحضور الملتقيات المتخصصة في المجال والاستفادة من الخبرات الدولية وتخصيص له دورات تكوينية وتدريبية. وهدا لا يتأتى إلا بتوفر إرادة وتكاثف وتظافر الجهود لرسم خارطة الطريق التي تسير عليها المنظمة من خلال إقرار سياسة شاملة لأمن المعلومات قابلة للتطبيق في أرض الواقع ومرنة قابلة للتعديل حسب طبيعة وثائق المؤسسة ونشاطها والمستفيدين منها.

9. قائمة المراجع:

1.9 باللغة العربية:

– الكتب:

1. القحطاني محمد عبد الله علي، خالد سليمان الغثبر، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات: الرياض، 2009 متاح على الرابط : books-library.online/free-1917333-download

2. أنجرس موريس، منهجية البحث العلمي في العلوم الإنسانية: تدريبات علمية. ط02، الجزائر، دار القصبة،2006.

3. خليفة شعبان عبد العزيز. المحاورات في مناهج البحث في علم المكتبات والمعلومات. مصر: الدار المصرية اللبنانية.1997

– المنشورات:

4. قذايفية أمينة، استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، المجلد 06، العدد01، متاح على المنصة الوطنية للمجلات الجزائرية ASJP على الرابط: https://www.asjp.cerist.dz/en/article/31120

5. فيلالي أسماء، شليل عبد اللطيف، تهديدات أمن المعلومات وسبل التصدي لها. مجلة البشائر الاقتصادية (المجلد الرابع، العدد 03)، 2017.

6. بشير، عماد: مسار الوثائق الإدارية ومعالجتها، كلية الإعلام والتوثيق، الجامعة اللبنانية، متاح على الخط: http://www.al-raeed.net/training

7. الصاحب، محمود حسن، سياسة أمن المعلومات في الجامعات: حالة دراسية (مجلة سيبارين ع33. ديسمبر 2013) متاح على: http//www.cybrarians.info/journal/n…o-secuirty.htm

8. حسني علي قاسم الشمالي، أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية في البنوك العاملة في الأردن. إدارة أعمال، كلية توليدو الأهلية، اربد، الأردن،2016.

9. الشيخ، خالد ياسين، أمن نظم المعلومات والرقابة (التحكم): ماجستير التأهيل والتخصص في الريادة والإدارة بالإبداع، الهندسة المعلوماتية بجامعة دمشق، 2015.

10. عزة فاروق جهري، طه محمد طه حسن، أمن المعلومات الرقمية وسُبل حمايته في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات، المجلد السادس – العدد 11، 2019.

11. مصطفى البكري، يوسف علي الشيخ، أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلى مكتبتي النيلين وجامعة وادي النيل Qscience proceeding.vol3.The SLA-AGC. 23rd Annual conference.2017 Available on : https://doi.org/10.5339/qproc.2017.gsla.3

2.9 باللغات الأجنبية:

12. Kolapati, V. *Cryptography and Security*. Disponible sur : mailto:http://dspace.cusat.ac.in/jspui/bitstream/123456789/2628/1/Cryptography%20and%20Security.pdf.

13. Siponen, M., Mahmoud, M. A., & Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2),2014.
14. Kolapati, V. *Cryptography and Security*. Disponible sur : mailto:http://dspace.cusat.ac.in/jspui/bitstream/123456789/2628/1/Cryptography%20and%20Security.pdf.
15. Campbell، T. *PRACTICAL INFORMATION SECURITY MANAGEMENT*. Apress.2017
16. Léopold. E, & Lhoste. S, la sécurité informatique. 3éme édition. 2007

***متفرقات:**

17. مقابلة مع مدير مشروع الرقمنة بتاريخ:2019/12/22 بمكتبه مديرية التربية لولاية قسنطينة.
18.شواو، عبد الباسط. محاضرات غير منشورة في مقياس المعايير والتقييس في الأرشيف. السنة الأولى ماستر تقنيات أرشيفية. جامعة قسنطينة02 عبد الحميد مهري. معهد علم المكتبات والتوثيق. الموسم الجامعي 2015/2014
19. وزارة التربية الوطنية، منشور رقم: 2018/230 الإطار المرجعي المتعلق بالنظام المعلوماتي لقطاع التربية الوطنية.
20. وزارة التربية الوطنية، المنشور رقم 1098 بتاريخ: 25 ماي 2017. ف/ي التدابير الوقائية ضد الهجومات الالكترونية (بخصوص فيروس Ransomware)
21. القانون 15-04 الخاص بالتوقيع والتصديق الإلكترونيين، متاح عبر http://www.joradp.dz/fta/jo-arabe/2015/a2015006.pdf تاريخ الزيارة: 2020./04/05
22. نشرة احصائية بمكتب الإحصاء بمديرية التربية لولاية قسنطينة للموسم الدراسي 2020/2019 .