أمن وحماية الوثائق الإلكترونية من خلال المعايير الدولية والنصوص التشريعية: دراسة تحليلية للمعيارين ISO 27001 و ISO 27002 والقانون 15-04 المتعلق بالتوقيع الالكتروني

Sécurité et protection des documents électroniques au moyen de normes internationales et de textes législatifs : une étude analytique des normes ISO 27001, ISO 27002 et de la loi 15-04 relative à la signature électronique

Security and Protection of Electronic Documents through International Standards and Legislative Texts: an Analytical Study to ISO 27001, ISO 27002 and the Law 15-04 Related to Electronic Signature

كحيلة سارة
الجزائر2 Alger

مقدمة

تعتبر الوثائق الإلكترونية من المقومات الأساسية التي تعتمد عليها الحكومة الإلكترونية، سواء كان ذلك في المؤسسات الحكومية أو القطاع الخاص، ونظرا لأهميتها وجب الاعتراف بمصداقيتها كما هو الحال عند نضيرتها الورقية، والاهتمام بها وحمايتها من جميع المخاطر التي قد تتعرض لها كالسرقة، التزوير، القرصنة، الفيروسات وغيرها من المخاطر.

هذا ما جعل المنظمات والهيئات الدولية تعمل على إصدار المعايير الخاصة بأمن وحماية الوثيقة الإلكترونية، لمساعدة مختلف المؤسسات والقطاعات الحكومية والخاصة على توفير أعلى درجات الأمن والحماية عند الاعتماد على نظم وبرامج إدارة الوثائق الالكترونية في مختلف مراحل التسيير الإداري، وفي هذا الإطار قامت المنظمة الدولية للتقييس بإصدار المعيارين ISO 27001 وISO 27002 والمتعلقين بتكنولوجيا المعلومات وتقنيات الأمن ونظم إدارة وحماية المعلومات وقواعد ممارسة أمن المعلومات.

وبالموازاة مع ذلك تسعى معظم الدول إلى مواكبة التحول نحو نظم إدارة الوثائق الالكترونية من خلال إصدار النصوص التشريعية اللازمة لذلك، وعلى هذا الأساس حاول المشرع الجزائري توفير الحماية اللازمة للوثيقة الالكترونية من خلال إصدار النص التشريعي المتمثل في القانون 15-04 الذي يحدد القواعد العامة للتوقيع والتصديق

الالكترونيين، والذي حدد آلية حماية الوثيقة الإلكترونية من خلال التوقيع الالكتروني، ومن هذا المنطلق جاءت الإشكالية الرئيسية للدراسة كما يلي:

- ما مدى مساهمة المعيارين ISO 27001 وISO 27002 والقانون 15-04 الذي يحدد القواعد العامة للتوقيع والتصديق الالكترونيين في أمن وحماية الوثائق الإلكترونية؟
- وتفصيلا للإشكالية الرئيسية يمكن طرح مجموعة من التساؤلات التالية:
- ما هو مفهوم الوثيقة الإلكترونية وما هي أهم المخاطر التي تتعرض لها؟
- ما هي طرق حماية الوثيقة الإلكترونية؟
- ما هو محتوى المعيارين ISO 27001 وISO 27002 وما هو دورهما في حماية الوثيقة الالكترونية؟
- كيف يساهم النص التشريعي 15-04 في حماية الوثيقة الإلكترونية في الجزائر؟

1. تعريف الوثيقة الالكترونية وأهداف الدراسة

1.1. أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف كالآتي:

- التعرف على أهم المخاطر التي تهدد الوثائق الإلكترونية وسبل حمايتها.
- التعريف بالمعايير الدولية الخاصة بأمن وحماية الوثائق الإلكترونية واستراتيجياتها في الحفاظ على الوثائق الالكترونية.
- التعرف على أهم التشريعات في الجزائر والتي تساعد في أمن وحماية الوثائق الالكترونية.
- التعرف على دور كل من المعايير والتشريعات في أمن وحماية الوثائق الإلكترونية.

2.1. تعريف الوثيقة الالكترونية

يعرف المجلس الدولي للأرشيف الوثيقة الإلكترونية بأنها كل المعلومات المسجلة الصادرة أو الواردة في نطاق إدارة نشاط رسمي أو شخصي، من بدايته إلى نهايته، التي تشمل محتوى ومحيط وهيكل لتبرهن على حقيقة النشاط، بغض النظر عن شكلها ووسائط تخزينها، وقد تكون هذه الوثائق في شكل مواقع أنترنت، وثائق صادرة عن معالجة النص بالكمبيوتر، قواعد البيانات والنصوص الفائقة، الصور والصفحات المنشورة، البرامج الحاسوبية، البريد الإلكتروني والشرائط المصورة...إلخ. (Mc Donald 2005:10)

كما جاء تعريفها بأنها مستندات تنتجها وتحفظها المؤسسات والإدارات في خضم النشاطات اليومية بصورة عفوية، بمساهمة تكنولوجيا المعلومات والاتصال، فهي تعالج

نواتج نشاطاتها وشواهد على وظائفها وأعمالها، على أن تتوفر في هذه الوثائق الشروط التالية:

- الأصالة (Authenticity).
- السلامة (Integrity).
- الثبوتية (Reliability).
- قابلية الاستعمال (Operability). (شعبان 2016: 80)

وتعرف الوثائق الالكترونية كذلك بأنها عبارة عن مادة (بيانات أو برامج) مشفرة للاستخدام بواسطة الحاسوب وقد يتطلب استخدام هذه المادة وجود طرفية مرتبطة مباشرة بجهاز الحاسوب (مثل مشغل الأقراص المدمجة) أو شبكة حاسوبية مثل شبكة الانترنت. (شاشة 2016: 157)

مما سبق يتضح أن الوثيقة الإلكترونية هي كل وثيقة تحتوي على معلومات مسجلة بواسطة الحاسب الآلي ومخزنة على وسائط إلكترونية، يتم معالجتها وإتاحتها باستخدام التقنيات الحديثة، وقد تكون في شكل صورة أو نص أو صوت أو أي شكل من أشكال المعلومات الإلكترونية.

2. أمن وحماية الوثيقة الالكترونية

تسعى مختلف المؤسسات والهيئات على جعل التعامل مع الوثائق الالكترونية بداية من الاقتناء إلى المعالجة والتخزين ثم الاتاحة، على درجة عالية من الأمن ووفق شروط الحماية اللازمة.

1.2. مفهوم أمن وحماية الوثيقة الإلكترونية

جاء مفهوم أمن وحماية الوثيقة الالكترونية بأنها السياسات والممارسات والتقنيات التي يجب توفيرها داخل المؤسسة لتداول المعلومات والوثائق عبر الشبكات بدرجة معقولة من الأمان، هذا الأمان ينطبق على عمليات المعالجة والتخزين الالكتروني. (Sadowsky 2003: 164)

كما يقصد به مجموع الإجراءات والقواعد والتشريعات التي توضع للحفاظ على سلامة وتكامل نظام المعلومات من التخريب والعبث والفقدان، وكذلك من التغيير والاستعمال غير المسموح به، سواء كان هذا التغيير أو التخزين مقصود أو غير مقصود. (عطيات 2004: 122)

يتضح مما سبق أن أمن وحماية الوثيقة الإلكترونية يتعلق بمجموع الإجراءات والعمليات التي تساعد على تجنيب الوثيقة كل العوامل التي تؤدي إلى فقدانها أو تعرضها

للمخاطر، من خلال حماية الحواسيب والنظم ووسائط التخزين وعمليات المعالجة وشروط الإتاحة.

2.2. المخاطر التي تتعرض لها الوثيقة الإلكترونية

تتعرض الوثيقة الإلكترونية إلى مجموعة من المخاطر في مختلف مراحل استخدامها، بداية من الاقتناء الرقمي، وصولا إلى المعالجة والتخزين والاتاحة وقد ذكر أشرف محمد عبده أهم هذه المخاطر والتي لخصها فيما يلي: (أشرف 2015: 283-284)

- الوصول غير المرخص إلى الأجهزة ووسائط التخزين وكذلك قواعد البيانات التي تعمل على تشغيل النظام سواء داخل أو خارج المؤسسة.
- التلف الذي يصاحب دخول الفيروسات أثناء انتقال المعلومات عبر قنوات ووسائل الاتصال المختلفة.
- تعطل الآلات والتجهيزات وتوقفها عن العمل بسبب عطل ميكانيكي أو عطل في البرمجيات.
- وجود بعض التجهيزات أو المحطات الطرفية في أماكن غير آمنة مما يجعلها عرضة للسرقة.
- عدم كفاية إجراءات أمن وحماية الوثائق الإلكترونية كأن تكون غير محمية بشكل كاف أو يكون من السهل على الغير اكتشاف آلية الحماية المستخدمة والقدرة على تعطيلها.

فالوثائق الالكترونية معرضة للعديد من المخاطر سواء تلك المتعلقة بالتجهيزات أو البرمجيات، أو عمليات القرصنة المنظمة، لذا وجب توفير أجود وأحسن طرق الحماية في ظل بيئة رقمية متطورة ومتغيرة باستمرار.

3.2. طرق وإجراءات حماية الوثيقة الإلكترونية

بغية توفير أحسن الشروط لحماية الوثيقة الالكترونية، وجب اتباع مجموعة من الخطوات والإجراءات نلخصها فيما يلي:

- استخدام البرامج المضادة للفيروسات (Les Antivirus) وتحديثها.
- فحص وسائط التخزين قبل استعمالها وعمل نسخ احتياطية للبرمجيات والملفات. (عطيات 2004: 151)
- استخدام الجدران النارية التي تقوم بتنظيم حركة البيانات والحفاظ على أمن الشبكات. (الجنيبهى 2005: 65)

- تشفير البيانات عند إرسالها عبر الشبكات وذلك بتحويلها إلى رموز غير مفهومة ودون معنى لمنع أي شخص غير مرخص له من الاطلاع عليها. (Stamp 2011: 492)
- اعتماد تقنية الكاشفات الإلكترونية والبيولوجية (تقنية الكشف عن ملامح الوجه، قزحة العين، الصوت، بصمة الأصبع، كف اليد)
- عدم الاحتفاظ بالبيانات الحساسة في الحاسب الآلي مثل البيانات المالية والشخصية خشية وقوعها بأيدي المخترقين.
- عدم استخدام البرامج المجانية غير الموثوق بها، لأن عددا كبيرا منها يقوم بتثبيت برامج التجسس وضرورة التأكد من اتفاقية الترخيص بشكل كامل قبل تثبيت أي برنامج. (الأرياني 2016: 48)

فاتباع الإجراءات السابقة مع تحديد أهم الأخطار التي تتعرض الوثيقة الالكترونية في مختلف مراحل استخداماتها، يساهم في حمايتها وسريتها وديمومتها للاستعمال على المدى البعيد.

3. المعايير الدولية لحماية الوثيقة الالكترونية

اهتمت المنظمة الدولية للتقييس بالتحول الحاصل نحو استخدام نظم وبرامج إدارة الوثائق الإلكترونية من طرف مختلف المؤسسات والهيئات، حيث قامت بوضع عدة معايير خاصة بالوثيقة الالكترونية؛ وضمت هذه المعايير مجالات الإدارة والتسيير، الأمن، الحماية والإتاحة، ومن هذه المعايير نجد المعايرين ISO 27001 وISO 27002 والذين تطرقا لآلية أمن وحماية الوثيقة الالكترونية.

1.3. معيار ISO27001 الخاص بنظم إدارة وحماية المعلومات (المتطلبات)

يحدد هذا المعيار المستلزمات الواجبة لتصميم ووضع نظام لتسيير أمن المعلومات من خلال توضيح مراحل الإعداد والاستغلال والمراقبة والتطوير، ويعطي المستلزمات الخاصة بالوثائق، وهو نظام إدارة متحكم لحماية المعلومات ويقلل من التهديدات التي تواجه جميع العمليات التجارية، والمراقبة والتحكم الفعال لمخاطر أمن المعلومات. ((ISO/CEI 27001: 2013

1.1.3. هيكلة المعيار

يعتمد هذا المعيار في عمله على تسعة أجزاء للمعالجة التي حددها تحالف صناعة حماية شبكات الانترنيت (CSIA) ويمكن تلخيصها كالاتي:

1. تعريف المجال لنظام إدارة حماية المعلومات(ISMS).
2. تعريف سياسة حماية المعلومات.

3. تقييم الأخطار/التحليل.
4. إدارة الخطر.
5. تحديد الأهداف للسيطرة والسيطرة الفعلية عليها / التطبيق.
6. تجهيز بيان (كشف) التطبيق.
7. تطبيق وتشغيل نظام إدارة حماية المعلومات.
8. استمرار المراقبة ومراجعة نظام إدارة حماية المعلومات.
9. إدامة وتحسين نظام إدارة حماية المعلومات. (Humphreys 2016 : 23-25)

فقد حاول هذا المعيار العمل على تحديد كل النقاط المهمة والتي يجب الاعتماد عليها عند انشاء واعتماد نظم لحماية المعلومات والوثائق الالكترونية داخل أي مؤسسة.

2.1.3. هدف المعيار

وهو يهدف إلى تحديد الاحتياجات اللازمة لتنفيذ وتشغيل وصيانة وتوثيق نظام إدارة أمن المعلومات داخل المؤسسة، ويتم تطبقه في أربعة مراحل:

- الخطة: تأسيس نظام لإدارة أمن المعلومات.
- التنفيذ: البدء في تنفيذ الخطط وتشغيلها.
- التحقق: مراجعة النظام بعد تنفيذه.
- العمل: صيانة وتحسين النظام. (الشريف 2016: 95)

فالتطبيق الفعال لهذا المعيار يساعد المؤسسات، في توفير درجة عالية من الحماية للوثائق الالكترونية، مما يقلل من احتمالية تعرضها للضياع والقرصنة، كما عملت المنظمة الدولية للتقييس على مواكبة التغييرات الحاصلة في المجال التكنولوجي من خلال العمل على إصدار معايير لاحقة مكملة لهذا المعيار.

2.3. معيار ISO27002: قواعد ممارسة أمن المعلومات

1.2.3. تعريف المعيار

هو معيار أكثر تفصيلا عن معيار ISO27001 لكونه يضع إرشادات وأسس عامة لبدء وتنفيذ إدارة أمن المعلومات وتحسينها والحفاظ عليها داخل المؤسسة، وحدد المعيار عدة تعاريف لأهم المصطلحات التي لها علاقة بوضع وتجسيد نظم إدارة أمن وحماية المعلومات والوثائق الالكترونية نذكر منها: (G. Ngqondi 2009: 32-33)

- أمن المعلومات: أي الحفاظ على سرية وسلامة وتوافر المعلومات.
- الخطر: مزيج من احتمال الحدث ونتيجته.
- تحليل المخاطر: الاستخدام المنهجي للمعلومات لتحديد المصادر ولتقدير المخاطر.

- تقييم المخاطر: عملية مقارنة المخاطر المقدرة مقابل معايير المخاطر المحددة.
- معالجة المخاطر: عملية اختيار وتنفيذ التدابير لتعديل المخاطر.

يوفر المعيار نصائح عامة حول الأهداف المقبولة لإدارة أمن المعلومات والوثائق، ويقوم بوضع مبادئ توجيهية لعملية تطوير معايير الأمن التقنية وإدارة الأمن الفعالة.

2.2.3. هيكلة المعيار

يحتوي المعيار على إحدى عشرة بندا للتحكم الأمني وهي كما يلي:

1. السياسة الأمنية.
2. تنظيم أمن المعلومات.
3. إدارة الوصول.
4. أمن الموارد البشرية.
5. الأمن المادي والبيئي.
6. إدارة الاتصالات والعمليات.
7. التحكم في الوصول.
8. اقتناء وتطوير نظم المعلومات.
9. إدارة حوادث أمن المعلومات.
10. إدارة استمرارية الأعمال.
11. الامتثال القانوني. (15-Béatrice Joucreau; Julien Levrard 2014: 09)

فالمعيار iso 27002 يحدد فئات الأمان الرئيسة التي تساعد على حماية الوثائق والمعلومات الالكترونية، ويتيح للمؤسسات العمومية والخاصة وحتى الأفراد بناء نظم الحماية التي تساعد على تحقيق أمن المعلومات وسريتها وتوافرها وسلامتها على المدى الطويل.

3.3. دور المعيارين ISO 27001 وISO 27002 في حماية الوثيقة الالكترونية

من خلال دراسة أهم ما جاء في المعيارين؛ فهما يساهمان في حماية الوثيقة الإلكترونية من خلال:

- وضع سياسة أمنية لحماية الوثائق الإلكترونية يمكن لكل مؤسسة أن تطبقها، قد تكون عبارة عن نظام أو برنامج أمني والتي من شأنها أن تحمي الوثائق من أي خطر.
- التحقق من تفعيل كل أجزاء السياسة الأمنية.

- تقييم المخاطر التي تتعرض لها الوثيقة الإلكترونية، وهذا يساعد المؤسسات في تحديد الحوادث المحتملة وتحديد مستوى الخطر.
- تحديد نقاط الضعف والقوة في أي برنامج أو نظام أمني ومحاولة تدارك ذلك ووضع تدابير للسلامة والوقاية من جميع الأخطار التي قد تتعرض لها الوثيقة الإلكترونية.
- وضع نظام إدارة وحماية المعلومات وهو مجموعة من السياسات والعمليات وإدارة المخاطر الخاصة بأمن المعلومات.
- تحديد الأبعاد الثلاثة لحماية المعلومات المتمثلة في السرية، التكاملية، التوافر، والتي تحمي الوثيقة الإلكترونية من السرقة أو التلاعب في محتوى البيانات أو فقدانها جراء عطل في أحد الأجهزة أو الأنظمة.
- وضع بنود التحكم الأمني الذي يساعد المؤسسات على تحقيق أهداف الامن والسلامة من خلال بناء نظام رقمي، لحماية المعلومات كأنظمة التشفير.

ومما سبق ومن خلال الدراسة التحليلية للمعيارين ISO 27001 وISO 27002 يتضح أن الاعتماد على المعايير الدولية لأمن وحماية الوثيقة الإلكترونية له العديد من نقاط القوة كما أنه لا يخلو من بعض نقاط الضعف والتي يمكن إجمالها فيما يلي:

1.3.3. نقاط القوة الواردة في المعيارين

- وضع تعريف لمجموعة من المصطلحات ذات العلاقة بأمن وحماية الوثيقة الإلكترونية.
- توضيح كيفية إنشاء نظام إدارة وحماية المعلومات(ISMS).
- تقييم الأخطار التي تتعرض لها الوثيقة الإلكترونية.
- توفير مجموعة من الجداول المساعدة على فهم كيفية تقييم المخاطر ومدى توافرها وسريتها.
- وضع دليل لحماية الوثائق الإلكترونية في المؤسسات الصغيرة والمتوسطة الرقمية.

2.3.3. نقاط الضعف الواردة في المعيارين ISO 27001 وISO 27002

نقاط الضعف الواردة في المعيارين هي:

- عدم التفصيل في المخاطر التي تتعرض لها الوثيقة الإلكترونية وسبل الوقاية منها.
- لم يتطرق المعيارين إلى التوقيع الإلكتروني الذي يعتبر من أهم أساليب حماية الوثيقة الإلكترونية.

- لم يحدد المعيارين أهم المعايير ذات العلاقة بهما، والتي من شأنها مساعدة المختصين في إعداد نظم وبرامج إدارة الوثائق الإلكترونية وتوفير الحماية اللازمة للوثيقة الإلكترونية.
- لم يدرجا بعض النماذج الخاصة بنظم وبرامج حماية الوثيقة الإلكترونية، لمساعدة المؤسسات على اقتناء النظم والبرامج الأكثر فعالية.

4. حماية الوثيقة الإلكترونية من خلال القانون 04-15 المتعلق بالتوقيع والتصديق الالكترونيين

يسعى المشرع الجزائري إلى مواكبة التطورات التكنولوجية الحديثة في مجال الإدارة، حيث تشهد السنوات الأخير توجه غالبية المؤسسات والقطاعات الوزارية إلى التوجه نحو الرقمنة واستخدام نظم إدارة الوثائق الإلكترونية، كما هو الشأن في وزارة العدل، وزارة التربية الوطنية، وزارة الداخلية، وزارة المالية ...، وغيرها من المؤسسات والقطاعات الوزارية وعلى هذا الأساس بادر بإصدار القانون 15-04 المؤرخ في 01 فبراير 2015 المتعلق بالتوقيع والتصديق الالكترونيين، حيث أعطى الصبغة القانونية لاستخدام التوقيع الالكتروني في مختلف مراحل التسيير الإداري وهذا ما ساهم في توفير العديد من السبل والخيارات لحماية الوثائق الالكترونية من مختلف المخاطر التي تهددها.

1.4. محتوى القانون 04-15 المتعلق بالتوقيع والتصديق الالكترونيين

يتضمن هذا النص التشريعي المتعلق بالتوقيع والتصديق الالكترونيين في الجزائر 10 فصول موزعة على خمسة أبواب؛ (القانون 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين 2015: 06-16)

1. الباب الأول : تضمن الباب الأول ثلاثة فصول :

- حيث جاء في الفصل الأول هدف القانون وهو تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.
- أما الفصل الثاني فتضمن التعاريف القانونية للمصطلحات ذات العلاقة بنص هذا القانون، ومما جاء فيه أن التوقيع الالكتروني عبارة عن بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق،
- أما الفصل الثالث فحدد فيه المشرع الجزائري المبادئ العامة للتوقيع الإلكتروني.

2. الباب الثاني : أما الباب الثاني فتضمن فصليين؛

- 1حيث حدد الفصل الأول متطلبات التوقيع الالكتروني وهي؛ أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة، وأن يرتبط بالموقع دون سواه، وأن

يكون مرتبطا بالبيانات الخاصة به ويمكن من تحديد هويته، وأن يكون مصمما بواسطة آلية مؤمنة، وبوسائل تكون تحت التحكم الحصري للموقع.

- أما الفصل الثاني فتضمن آليات إنشاء التوقيع الإلكتروني والتحقق منه، وشروط إنشاء هذه الآلية، والتي حددها القانون في:
- وجوب أن تضمن هذه الآلية بواسطة الوسائل التقنية والإجراءات المناسبة، ما يلي:
- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة.
- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنساخ وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد.
- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.
- يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع.

3. الباب الثالث : أما الباب الثالث فتناول فيه المشرع التصديق الإلكتروني، وتضمن أربع فصول:

- الفصل الأول تناول شهادة التصديق الإلكتروني الموصوفة.
- الفصل الثاني: يتناول سلطات التصديق الإلكتروني، وضم ثلاث أقسام،
- حيث تناول القسم الأول السلطة الوطنية للتصديق الالكتروني، وأشار إلى أنه تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، كما حدد مهامها.
- أما القسم الثاني فتضمن السلطة الحكومية للتصديق الالكتروني، كما قام بتحديد مهامها.
- أما القسم الثالث فتضمن السلطة الاقتصادية للتصديق الإلكتروني، والمهام المنوطة بها.
- فيما تناول الفصل الثالث من الباب الثاني، النظام القانوني لتأدية خدمات التصديق الإلكتروني، حيث تطرق إلى مؤدي خدمات التصديق الإلكتروني ومسؤولياتهم، وتناولت المادة 34 من الشروط التي تتوفر في طالب الترخيص لتأدية خدمة التوقيع الإلكتروني والمتمثلة في:

- أن يكون خاضعا للقانون الجزائري للشخص المعنوي أو الجنسية الجزائرية للشخص الطبيعي، وأن يتمتع بقدرة مالية كافية.
- أن يتمتع بمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال للشخص الطبيعي أو المسير للشخص المعنوي.
- أن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني.

4. الباب الرابع :أما الباب الرابع تضمن فصليين حيث جاء في الفصل الأول منه العقوبات المالية والإدارية المترتبة عن عدم احترام مؤدي خدمات التصديق الالكتروني لأحكام دفتر الشروط أو سياسة التصديق الالكتروني الخاصة به، أو في حالة انتهاك مؤدي خدمات التصديق الالكتروني للمقتضيات التي يتطلبها الدفاع الوطني، وتناول الفصل الثاني الأحكام الجزائية، حيث يعاقب بالحبس وبغرامات مالية كل من لم يحترم الشروط التي جاءت في نص القانون حسب ما أوضحته المواد من 66 إلى 75 منه.
5. الباب الخامس :وأخيرا الباب الخامس فهو عبارة عن أحكام انتقالية وختامية.

2.4. دور القانون 04-15 في حماية الوثيقة الإلكترونية

من خلال تحليل القانون 15-04 فهو يساهم في حماية الوثيقة الإلكترونية من خلال:

1. إعطاء مصداقية للوثيقة الإلكترونية واعتبارها وثيقة رسمية، من خلال الاعتراف بالتوقيع الإلكتروني.
2. التوقيع الإلكتروني يحمي الوثيقة الإلكترونية من أشكال التزوير والتحريف والسرقة ولا ينسبها إلا لمنشئها الأصلي.
3. تحديد سلطات التوقيع الإلكتروني التي من شأنها أن تقوم بإعداد سياسة التصديق الإلكتروني، إضافة إلى مجموعة من المهام الموكلة إليها والمتعلقة بالجهة التابعة لها.
4. وضع النظام القانوني لتأدية خدمات التصديق الإلكتروني.
5. وضع الأحكام الجزائية من خلال المعاقبة بالسجن وبغرامات مالية كل من؛

- يؤدي بقرارات كاذبة للحصول على شهادة التصديق الإلكتروني.
- من يقوم بحيازة وإفشاء أو استعمال بيانات إنشاء التوقيع الإلكتروني الخاصة بالغير.
- كل من يؤدي خدمات التصديق الإلكتروني ولا يحافظ على سرية البيانات المتعلقة بشهادات التصديق الإلكتروني الممنوحة، وجمه بيانات المعني دون موافقته.

- استعمال شهادة التصديق الإلكتروني لغير الأغراض التي منحت له.
- 3.4. نقاط القوة ونقاط الضعف المتعلقة بحماية الوثيقة الالكترونية الواردة في النص التشريعي 15-04

ومما سبق ومن خلال دراسة مضمون القانون 15- 04 الخاص بالتوقيع والتصديق الالكترونيين، فإن التقيد بهذا النص في أمن وحماية الوثيقة الإلكترونية له العديد من نقاط القوة وبعض نقاط الضعف والتي نوجزها فيما يلي:

1.3.4. نقاط القوة المتعلقة بحماية الوثيقة الالكترونية الواردة في النص التشريعي 15-04

حاول المشرع الجزائري مواكبة التطورات الحاصلة التي أحدثتها تكنولوجيا المعلومات والاتصال، وزيادة توجه مختلف المؤسسات والإدارات العمومية نحو استخدام نظم إدارة الوثائق الالكترونية، وتمثلت نقاط القوة الواردة في النص التشريعي 15-04 كما يلي:

- التعريف بأهم المصطلحات ذات العلاقة بالتوقيع الإلكتروني.
- تحديد سلطات التصديق الإلكتروني والمهام الموكلة إلى كل سلطة.
- تعيين مؤدي خدمات التوقيع الإلكتروني وأدواره ومسؤولياته.
- تحديد سياسة التصديق الإلكتروني ومسؤوليات الموقع، والتطرق إلى مشروعية التوقيع الإلكتروني الخارجي، وذلك من خلال اتفاقية الاعتراف المتبادل الذي أبرمته الدولة.

2.3.4. نقاط الضعف

على الرغم من كون النص التشريعي 15-04 المتعلق بالتوقيع والتصديق الالكترونيين يسعى إلى حماية الوثيقة الالكترونية من خلال إعطاءها الصبغة القانونية في مختلف التعاملات، إلا ان هذه النص له العديد من نقاط الضعف، نلخصها فيما يلي:

- لم يتطرق القانون إلى أشكال التوقيع الإلكتروني المعترف بها لإثبات مصداقية الوثيقة الإلكترونية.
- لم يحدد القانون حقوق الموقع، وكيفية تعويضه في حالة تعرض توقيعه للسرقة أو التزوير.
- المشرع الجزائري لم يذكر شروط التوقيع الإلكتروني وإجراءاته.
- لم يتم الإشارة في هذا القانون إلى دور التوقيع الإلكتروني في إبرام المعاملات التجارية.

خاتمة

يتزايد يوما بعد يوم الاعتماد على الوثائق الالكترونية في مختلف مراحل التسيير الإداري، ولتوفير الشروط الضرورية لأمن وحماية الوثائق الإلكترونية وجب الاعتماد على المعايير الدولية والنصوص التشريعية، لمواجهة المخاطر التي تتعرض لها ومواكبة التحديات التي تواجهها في ظل بيئة رقمية متغيرة ومتطورة باستمرار، ومن خلال دراستنا للمعيارين ISO 27001 وISO 27002 والنص التشريعي 15-04 توصلنا لمجموعة من النتائج اهمها:

- أن المعيارين ISO 27001 وISO 27002 لهما دور كبير في حماية الوثيقة الإلكترونية من خلال وضع سياسة أمنية لحمايتها، وتحديد خطوات بناء نظام ادارة حماية المعلومات.
- يساهم القانون 15-04 الخاص بالتوقيع والتصديق الالكترونيين في حماية الوثيقة الالكترونية، من خلال إعطاء صفة الرسمية للوثيقة الإلكترونية واستعمالها في النشاط الإداري داخل المؤسسات والإدارات العمومية والخاصة، إضافة إلى تعيين سلطات التوقيع الالكتروني وتحديد مهامها وآلية حماية الوثيقة الالكترونية من خلال التوقيع والتصديق الالكترونيين.

ومن أجل استخدام فعال للوثائق الالكترونية في مختلف المؤسسات والهيئات العمومية والخاصة نقترح ما يلي:

- تشجيع المؤسسات والإدارات العمومية نحو استخدام نظم وبرامج إدارة الوثائق الالكترونية وهذا للإيجابيات والمزايا التي تتيحها.
- الاعتماد على المعايير الدولية الخاصة بحماية الوثائق الإلكترونية عند بناء نظم إدارة الوثائق، خاصة منها المعياران iso 27001 وiso27002.
- الاعتماد على التوقيع الالكتروني في حماية الوثيقة الالكترونية تماشيا مع النص التشريعي 15-04 المتعلق بالتوقيع والتصديق الالكترونيين.
- تكوين القائمين على إدارة مشاريع الرقمنة وإدارة الوثائق الالكترونية في المؤسسات والإدارات العمومية على آلية حماية الوثائق الالكترونية من خلال المعايير الدولية والنصوص التشريعية وهذا من خلال برامج التكوين المستمر.

نشر الوعي المعلوماتي والثقافة الرقمية في المجتمع وتشجيع المستفيدين على استخدام الوثائق والخدمات الالكترونية لتحقيق حاجياتهم.

Humphreys Edward. . (2016) *Implementing the ISO/IEC 27001 ISMS Standard*. London: ARTECH HOUSE.

Joucreau Béatrice et levrard Julien. (2013). *ISO 27001:2013*. . 20 دادرتسالا خيرات 2020 mai، نم:https://www.gsdays.fr/IMG/pdf/conf-beatrice-joucreau_claire-carre.pdf

Mcdonald Andrew et autres. (2005). *Les archives Electronique: Manuel à l'usage des Archevistes*. Paris: Consiel International Des Archives .

Ngqondi Tembisa G. The ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards: A Comparative Analysis from a Healthcare Perspective (2009)..25 دادرتسالا خيرات mai, 2020،نم https://core.ac.uk/download/pdf/145049474.pdf

Sadowsky George. (2003). *Information Technology Security*. Washington: The World Bank. ISO. (2013). *ISO/CEI 27001:2013*. . 15mai, 2020،نم: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:fr

Stamp Mark.(2011) . *Information Security: Principles and Practice*. New Jersey: John Wiley and Sons, inc, hoboken.

أروى يحي الأرياني. (2016). الأعمال الالكترونية وتطبيقاتها. عمان: دار الوراق للنشر والتوزيع.

أشرف عبد المحسن الشريف. (2016). أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية. مجلة اعلم، الصفحات 87-114.

الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية. (2015). القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين. الجزائر.

جمال شعبان. (2016). الأرشيف الإداري الرقمي أساس الأرشفة الإلكترونية. مجلة اعلم، الصفحات 73-82.

عبد الرحمان شعبان عطيات. (2004). أمن الوثائق والمعلومات. عمان: الأكاديميون للنشر والتوزيع.

فارس شاشة. (2016). الوثيقة الرقمية: إعادة تعريف في ظل البيئة الالكترونية. مجلة علم المكتبات، الصفحات 153-176.

منير محمد الجنيبهى؛ ممدوح محمد الجنيبهى. (2005). أمن المعلومات الالكترونية. الإسكندرية: دار الفكر الجامعي.

مستخلص

تهدف هذه الدراسة إلى التعريف بالوثيقة الالكترونية وتوضيح الدور الذي تلعبه المعايير الدولية والنصوص التشريعية في أمنها وحمايتها، وهذا من خلال دراسة تحليلية للمعيارين ISO 27001 و ISO 27002، وتوضيح طرق أمن وحماية الوثيقة الالكترونية من خلالهما، كما تتناول تحليل القانون 15-04 الذي يحدد القواعد العامة للتوقيع والتصديق الإلكترونين في الجزائر، وتوضيح آلية حماية الوثيقة الإلكترونية من خلال إعطاء مصداقية للتوقيع الإلكتروني.

وتوصلت الدراسة إلى مجموعة من النتائج سمحت لنا بوضع بعض الاقتراحات الخاصة والتي تساهم في تحقيق أمن وحماية الوثيقة الإلكترونية.

كلمات مفتاحيّة

الوثيقة الإلكترونية؛ أمن وحماية الوثائق الإلكترونية؛ المعيار ISO27001، المعيار ISO27002، القانون 15-04، التوقيع الالكتروني.

Résumé

Cette étude vise à introduire le document électronique et à clarifier le rôle que jouent les normes internationales et les textes législatifs dans leur sécurité et leur protection et ce à travers une étude analytique des normes ISO27001 et ISO27002, et la clarification des méthodes de sécurité et de protection du document électronique à travers elles.

L'analyse de la loi 15-04, qui définit les règles générales de signature et d'authentification électroniques en Algérie, met en lumière le mécanisme de protection d'un document électronique en donnant foi à une signature électronique.

L'étude a abouti à un ensemble de résultats important pour assurer la sécurité et protection du document électronique.

Mots-clés

document électronique ; sécurité et protection des documents électronique ; norme ISO27001 ; norme ISO27002 ; loi 15-04 ; signature électronique.

Abstract

This study aims to introduce the electronic document and clarifies the role that international standards and legislative texts play in their security and protection, through an analytical study of ISO 27001 and ISO 27002, It clarifies the methods of security and protection of the electronic document through them.

Analysis of law 15-04, which defines the general rules for electronic signature and authentication in Algeria, sheds light on the mechanism for protecting an electronic document by giving credence to an electronic signature,

The study led to an important set of results to ensure the security and protection of the electronic document.

Keywords

electronic document, security and protection of electronic document, ISO27001, ISO27002, Law 15-04, electronic signature.