أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية

د. أشرف عبد المحسن الشريف

أستاذ مساعد الوثائق والمعلومات

جامعة بنى سويف

الملخــص:

تناول هذا البحث موضوع أمن وحماية المستندات الالكترونية التي يتم استخدامها من خلال الحكومات الالكترونية العربية ، وهناك اتجاه عام في معظم دول العالم الى تقديم الخدمات الحكومية الى الأفراد والمؤسسات العامة عبر الحكومة الالكترونية ، وناتج هذه الخدمات هو المستندات الالكترونية التي اذا ما تم الكشف عنها أو سرقتها عبر شبكات الحاسب سوف يؤدي الى اضرار كبير للأفراد أو المؤسسات ،لذا جاء هذا البحث ليوضح ماهية المستندات الالكترونية وخصائصها ، وبيان المخاطر التي تتعرض لها المستندات الالكترونية على شبكات المعلومات سواء كانت مخاطر خارجية أو داخلية ، وكذلك بيان طرق حماية المستندات الالكترونية باستخدام التقنيات الآلية أو الاجراءات الادارية ،وأخيرا يبين البحث نموذجا عمليا لحماية المستندات الالكترونية وهو بوابة حكومة إمارة أبو ظبي الالكترونية وبيان طرق تأمين وحماية مستنداتها الالكترونية والطرق التي تتبعها في مواجهة المخاطر تهدد المعلومات الحكومية والمستندات الالكترونية.

تمهيــد:

يعد المستند الإلكتروني الأداة الرئيسية لتنفيذ فكرة الإدارة الالكترونية التي يشاع تسميتها بالحكومة الالكترونية،إذ أنها تقضي باستخدام نظم المعلومات الرقمية في إنجاز المعاملات الإدارية وتقديم الخدمات والتواصل مع المواطنين بمزيد من الإفصاح والشفافية،فعن طريق الحكومة الالكترونية يتم التعامل مع الأجهزة الحكومية بسهولة ويسر من خلال الاتصال بالمواقع الخاصة بالوزارات والمؤسسات التابعة لها،فالشخص الطبيعي أو المعنوي يمكنه التعامل مع الضرائب والتعليم والمرور والبنوك،وخير مثال على ذلك ما ظهر حديثا من أنظمة مالية جديدة للوفاء بالالتزامات عن طريق الوسائل الالكترونية أو الدفع الالكتروني .

والمستند الإلكتروني هو المعلومات التي يتم انشاؤها أو ارسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية أو البريد الالكتروني أو البرق أو التلكس أو النسخ البرقي الفاكس. (عثمان الصديق احمد محمد , 2009).

أو هو كل سجل أو مستند يتم انشاؤه وتخزينه واستخراجه ونسخه وإرساله وابلاغه واستلامه بوسيلة الكترونية، على وسيط ملموس أو على أي وسيط الكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه. وقد تبنى القانون المصري التعريف الوارد في قانون الاونسترال النموذجي للتجارة الالكترونية ووصفه بانه رسالة بيانات الكترونية أو رقمية او ضوئية تخزن او ترسل او تستقبل كليا او جزئيا بوسيلة الكترونية او رقمية او ضوئية أو باي وسيلة اخرى مشابهة. ولقد نص المشرع الفرنسي على ان الكتابة التي تتم بهذه الصورة، لها الحجية الكاملة في الاثبات، شانها شان الكتابة التقليدية على دعامة ورقية، حسبما ورد في نص المادة 1/1316من القانون المدني الفرنسي وبشرط وحيد هو ان يكون حفظها قد تم في ظروف تضمن كمالها. (عمار كريم ناظم. 2007)

اما الحكومة الالكترونية فيقصد بها الخدمات الحكومية عبر الإنترنت، وقد يقصد بها الإدارة العامة الإلكترونية، ويمكن تعريفها بشكل أشمل بأنها تلك الحكومة التي تهدف إلى تقديم الخدمات الحكومية على اختلافها عبر الوسائط الإلكترونية وأدوات التكنولوجيا وأهمها الإنترنت والاتصالات فالحكومة الإلكترونية هي النسخة الافتراضية للحكومة الحقيقية الكلاسيكية مع فارق أن الأولى تعيش في الشبكات وأنظمة المعلوماتية والتكنولوجيا وتحاكي وظائف الثانية التي تتواجد بشكل مادي في أجهزة الدولة. (عمار كريم كاظم , 2007).

وتوفر الحكومة الالكترونية للأشخاص الدخول إلى قاعدة البيانات المخزونة على شكل ملفات لدى الدولة والمعنية بشؤون العاملين أو العملاء ، لذا فان المتعامل يستطيع الاطلاع على الوثائق أو الشهادات سواء كانت مخزنة على شكل مستندا الكتروني أم معلومات مجردة منطقيا ، ما عدا المعلومات التي يكون الاطلاع عليها يشكل اعتداءا على مصالح أساسية مثل المساس بسرية الحياة الخاصة للأشخاص وسرية معاملاتهم والمستندات المثبتة لها .

وبما أن المستند الالكتروني هو احد أدوات تنفيذ الحكومة الالكترونية التي تتميز بسرعة الانجاز ، فان إنشاء المستند قد لا يتجاوز دقائق معدودة ، مما يؤدي بدوره إلى توفير الوقت الضائع في الانتقال إلى مقر الإدارة وانجاز المعاملة يدويا ، لذا فأن استخدام الحكومة الالكترونية في إنشاء المستند الالكتروني أدى إلى الاستغناء عن خدمات بعض المرافق كخدمة المرفق البريد العادي ، الذي استعيض عنه بخدمة البريد الالكتروني E-Mail. (عمار كريم كاظم , 2007)

ووفقًا لتقرير "فروست أند سوليفان" الذي أزيح الستار عن نتائجه في الدورة الثانية لمعرض ومؤتمر الخليج لأمن المعلومات الذي أقيم في مركز دبي التجاري العالمي خلال المدة ما بين 9 و 11 حزيران/يونيو الحالي، يتوقع أن يصل الإنفاق في قطاع خدمات أمن تقنية المعلومات بدولة الإمارات العربية المتحدة إلى 1.7 مليار درهم (أي ما يعادل 473 مليون دولار) بحلول عام 2018 وبنسبة نمو تبلغ 17 بالمئة , مما يبين مدى اهتمام دول الخليج العربي وبصفة خاصة دولة الامارات العربية في حماية وتأمين المعلومات في المؤسسات الحكومية أو الخاصة على السواء.(البوابة العربية للأخبار التقنية , 2014).

أهداف البحث:

تهدف هذه الدراسة الى:

1- التعريف بأمن المستندات الالكترونية وحمايتها من خطر الانتهاك العمدي أو غير المتعمد.
2- توضيح العلاقة بين المستندات الالكترونية والحكومة الالكترونية.
3- بيان أهم المعايير الدولية التي تتعلق بأمن المستندات الالكترونية.
4- بيان أنواع المخاطر التي تهدد امن المعلومات وانتهاكها.
5- بيان أساليب وطرق حماية المستندات الالكترونية من خطر السرقة أو التطفل.
6- توضيح سياسة أمن وحماية المعلومات على بوابة الحكومة الالكترونية بإمارة أبو ظبي كنموذج يحتذى به في الدول العربية.

أسئلة البحث:

1- ما هي ماهية المستند الإلكتروني؟
2- هل توجد علاقة بين المستند الإلكتروني والحكومة الالكترونية؟
3- هل هناك معايير دولية لتحقيق أمن المستندات الالكترونية؟
4- ما هي الاساليب والطرق المتبعة لحماية أمن المستندات الالكترونية؟
5- ما هي انواع المخاطر التي تهدد أمن المستندات الالكترونية؟
6- كيف تواجه الادارات خطر انتهاك المستندات الالكترونية؟
7- ما هى الإجراءات تتخذها حكومة امارة ابو ظبي الالكترونية لحماية امن المعلومات؟

منهجية البحث:

اعتمد البحث على نوعين من المناهج هما:

أولا/ المنهج الوثائقي:

الذي يقوم على وصف الظاهرة المتمثلة في تأمين وحماية المستندات الالكترونية على بوابة أبو ظبي الالكترونية والعمل على تفسيرها وتوضيح أسبابها، من خلال جمع مصادر المعلومات المعاصرة عن الظاهرة (احصاءات، سجلات، كتب مطبوعة أو رقمية ....) والعمل على تحليلها للوصول الى نتائج يمكن تعميمها.

ثانيا/ منهج دراسة الحالة:

وهو دراسة رأسية متعمقة عن الظاهرة المتمثلة فى تأمين وحماية المعلومات الرسمية على موقع بوابة حكومة ابو ظبي الالكترونية ودراسة تفاصيل السياسة التي تتبعها لحماية وتأمين المعلومات على موقع البوابة.

كما تم استخدام اسلوب تحليل المضمون داخل منهج دراسة الحالة من خلال دراسة موقع بوابة حكومة ابو ظبي الالكترونية، والذي يعمل على تجميع وتحليل البيانات من اجل التوصل الى خصائص ومواصفات الظاهرة بغرض تفسيرها والوصول الى مؤشرات تساعد على فهمها.

وقد اختار البحث بوابة الحكومة الالكترونية لأمارة ابو ظبي بدولة الامارات العربية كنموذج للبوابات العربية وذلك للأسباب الآتية: -

1- أشار تقرير الأمم المتحدة للحكومة الإلكترونية الذي صدر في 2012 إلى تقدم دولة الإمارات إلى المركز السابع في خدمات الحكومة الإلكترونية، حيث قفزت الدولة 92 نقطة.
2- كما حلت حكومة دولة الامارات الالكترونية في المركز 28 في معيار الحكومة الإلكترونية على مستوى العالم.
3- بينما احتلت دولة الإمارات العربية المتحدة المرتبة الأولى خليجياً وعربياً في معيار الجاهزية الإلكترونية، جاءت مملكة البحرين في المرتبة 36 والمملكة العربية السعودية في المرتبة 41 ودولة قطر في المرتبة 48.

الدراسات السابقة:

تم الاعتماد على المصادر التالية في رصد الدراسات السابقة:

- البحث في موقع المجلس الأعلى للجامعات للوصول إلى الدراسات السابقة العربي سواء المجازة أم التي قيد التسجيل.

- البحث في محرك بحث Google، للوصول إلى دراسات العربية.
- البحث في قاعدة بيانات Proquest Digital Dissertation من خلال المجلس الأعلى للجامعات.

وفيما يلي عرض لأهم هذه الدراسات:

1- أمن الوثائق والمعلومات. عبد الرحمن شعبان عطيات , جامعة الامير نايف للعلوم الامنية , الرياض , 2004 ،.ويعتبر من أهم الكتب التي تتناول الأمن المكتبي المتعلق بكيفية حفظ المعلومات والوثائق ، ويأتي هذا الكتاب مواجهة لمختلف أنماط جرائم التجسس التي تتطلب تكريس الجهود العلمية والأمنية والقضائية لمواجهتها والحد من آثارها وتناول هذا الكتاب المكون من الموضوعات التالية:

1-الوثيقة: أنواعها، أهميتها، حفظها، أنماط المكافحة، الوثائق المحروقة.

2-الحبر: قواعد عامة، فحص الوثيقة، الحبر. - التزوير المادي في الوثائق والمستندات: التزوير، إزالة المعلومات.

3-كشف التزوير: كشف الإزالة، المحو والكشط، الإزالة الكيميائية. - الحماية من التزوير. - كشف التزييف والحماية منه.

4-حماية الوثائق. - أمن المعلومات والوثائق الإلكترونية.

وقد ركزت هذه الدراسة على أمن الوثائق الورقية أكثر من تركيزه على أمن الوثائق الإلكترونية، الا في الفصل الرابع الذي تناول أمن الوثائق الالكترونية دون تناول حمايتها على بوابة الحكومات العربية.

2. خالد عطيه محمد الزعفراني.- نموذج مقترح لتقييم أداء خدمات الحكومة الإلكترونية في جمهورية مصر العربية: دراسة تطبيقية.- صديق محمد عفيفي ، مني محمد إبراهيم البطل .- جامعة قناة السويس، كلية التجارة ببورسعيد : خالد ،2008.(أطروحة دكتوراه)

تهدف الدراسة إلى تقييم أداء الخدمة الإلكترونية المقدمة من جمهورية مصر العربية من أجل التوصل إلى نتائج يمكن الاستفادة بها عند وضع استراتيجية عامة لرفع مستوى الخدمات الإلكترونية المقدمة من حكومة جمهورية مصر العربية هذا إلى جانب تقديم مقترحات وتوصيات وبعض النماذج الإحصائية التي قد تفيد متخذي القرار لوضع حلول مستقبلية للخدمات الإلكترونية المقدمة من حكومة جمهورية مصر العربية، ولترشيد أساليب التقييم.

3.A study on electronic records management in electronic y. government. Wuhan university.

.Wu,juan il(2006). –

تناقش هذه الدراسة السجلات الالكترونية وإدارة الأرشفة في بيئة نظام الحكومة الالكترونية من خلال إلقاء الضوء على معنى شئون الحكومة الالكترونية والمفاهيم ذات الصلة علاوة على الفهم

الأعمق لنظام الحكومة الالكترونية وتحليل إطار العمل المتوافق من الجانب الالكتروني والجانب المعلوماتي، هذا إلى جانب دراسة السجلات الالكترونية في بيئة شئون الحكومة الالكترونية وتحليل متطلبات النظام وينظم وينفذ الخطوات الضرورية لإدارة السجلات الالكترونية، إضافة إلى تحليل العمل الأرشيفي لاسيما ذلك المتعلق بنظرية وتدفق العمل في نظام شئون الحكومة الالكترونية وإدارة التدفق الأرشيفي والحفظ في نظام إدارة المعلومات الأرشيفية. متناولا أيضاً متطلبات نظام إدارة المعلومات الأرشيفية وبناء سجلات الكترونية ومركز للسجلات الأرشيفية ويناقش مشكلات حفظ وتبادل البيانات في بيئة الحكومة الالكترونية.

Australian Government: Department of Defense (Intelligence and Security) .

Information Scurity Manual, 2014.

والغرض من هذا الدليل هو مساعدة وكالات الحكومة الأسترالية في تطبيق المنهج القائم على حماية المعلومات وأنظمتها. وتهدف هذه المبادئ التوجيهية لحماية المعلومات والنظم، وتقديم المشورة في هذا الدليل تستند بشكل خاص على تجربة مركز أمن المعلومات بوزارة الدفاع الأسترالية في توفير أمن المعلومات والمشورة ومساعدة الحكومة الأسترالية. لذا فقد تم في هذا الدليل تصميم الضوابط للتخفيف من معظم التهديدات المحتملة للوكالات الحكومية الأسترالية.

متن البحث:

أولا/تعريف المستند الإلكتروني:

كما يعرف أمن المعلومات الحكومية (المستند الإلكتروني) على أنه حماية المعلومات من التهديدات، ويتحقق من خلال الحفاظ على سرية وصحة وتوافر المعلومات:

- سرية المعلومات: هي فرض قيود مصرح بها على الدخول الى المعلومات والافصاح عنها ، ويتضمن هذا العمل تفير وسيلة لحماية الخصوصية الشخصية معلومات الملكية .
- صحة المعلومات: هي الوقاية ضد تعديل وإتلاف المعلومات وتتضمن ضمان عدم خرق المعلومات وضمان صحتها.
- توافر المعلومات: هي ضمان الدخول الى المعلومات واستخدامها بشكل موثوق وفى الوقت المناسب. ويساعد أمن المعلومات وفقا لهذه الأمور، وعلى سير عمل الخدمات الحكومية بدون عراقيل والقدرة على الحفاظ على " الاعمال كالمعتاد " .

وقد وضع المجلس الدولي للأرشيف ICA للمستند الإلكتروني صفات ثلاثة هي:

1. **المحتوى Content:** وهو الموضوع الرئيسي التي تدور حوله الوثيقة وأنشئت من أجله ويتفرع منه موضوعات فرعية.

2. **السياق Context:** وهي البنية التي أخرجت وأنتجت الوثيقة أي السياق الإداري المحيط بالوثائق بدءًا من الإدارة المنشئة وتاريخها وعلاقتها بالوثائق الأخرى ذات الصلة.

3. **البناء Structure:** وهي البيانات التي تساعد في تحديد ذاتية الوثيقة كالفصول وأجزاء الوثيقة والهوامش والفصول والأجزاء التي تتعلق بالبنية المنطقية للوثيقة وهي الرموز والمعطيات التي تساعد في تشكيله(international council Archive , 2004 , p.12-13)

وإذا ما توافرت هذه الصفات للمستند الإلكترونية فإنها تحقق لها ما يلي:

1. المصداقية حتى يمكن الاعتماد عليها عند اتخاذ القرارات.
2. التكامل وذلك لكي يتم التأكد من أن البيانات لن تتغير بشكل متكرر.
3. عدم الإنكار لمنع مُنشئ الوثيقة من التبرؤ منها Public records office , 2004 , p.12-13)

ثانياً/ مميزات المستندات الإلكترونيــة:

نظرًا للتطور التقني في مجال الوثائق والمعلومات أصبحت المؤسسات الحكومية تعتمد بشكل أساسي على توظيف التقنية في أداء أعمالها اليومية حيث تنتج المؤسسات الحكومية المزيد من الوثائق في أشكال إلكترونية مختلفة لها قيمتها ولابد من تحمل مسئولية تنظيمها وحفظها إلكترونيًا وتأتي الوسائط التقنية لتساهم بشكل فعال في إنتاج ونقل وحفظ واسترجاع الوثائق وجزء كبير من تلك المستندات الإلكترونية له قيمة دائمة تم استخدامها خلال فعاليات وأنشطة المؤسسات الحكومية من أجل اتخاذ القرارات لذلك لابد من حفظها وتنظيمها،لذا ينبغي تحديد سمات وخصائص تلك المستندات حتى يمكن لنا تحقيق إدارة فعالة لها ومنها: **.(قاسم أبو حرب ،2003،ص4):**

- إمكانية نقل المستندات من مكان لآخر فيمكن إرسالها بالبريد الإلكتروني إلى عدد لا يحصى من المستخدمين وبتكلفة ووقت أقل.
- قدرتها الهائلة على التنوع وخاصة فيما يتعلق بمجال البرامج غير النصية كالرسوم البيانية والتصميمات والصور والبرامج الخاصة بالتعليم والتدريب.
- سرعة الاسترجاع وسهولة الاستخدام بحيث يمكن استرجاعها بسهولة خلال ثوان معدودة بدلا من عدة دقائق وكذلك لعدد من الأشخاص قراءة الوثيقة نفسها أو رؤية الصورة نفسها في نفس الوقت. **(أحمد الكبيس , 2008, ص 4)**
- تخزن في أنواع متعددة من وسائط التخزين مثل الأقراص الصلبة والممغنطة وأقراص DVD ... الخ.

- تكون السيطرة على وسائط التخزين المخزنة عليها المستندات الالكترونية أسهل وأكثر دقة وفعالية من حيث تنظيم البيانات والمعلومات وحفظها وتحديثها مما ينعكس على كفاءة الوصول إليها(Alan, Howell , 2004 ,p.4)
- بعض الوثائق قد تكون أكثر فائدة وأهمية في الشكل الإلكتروني في نتيجة لتعزيز ودعم القرارات والمعالجة والتجهيز
- اقتصادية الاختزان فالزيادة في تكلفة حفظ المواد الورقية يجعل الأشكال الإلكترونية أكثر جاذبية من وجهة نظر اقتصادية (**شريف كامل شاهين**، 2000،ص 157)

ثالثا/ مفهوم أمن وحماية الوثائق الإلكترونية:

ينبغي على المنظمات أن تتأكد من الإبقاء على وثائقها الإلكترونية وحفظها متاحة ومقروءة مفهومة طوال الوقت بغض النظر عن الوسيط المخزنة عليها، وعلى الرغم مما تقدمه النظم الإلكترونية من مزايا مهمة للمنظمات، إلا أن التحديث المستمر والدوري لقواعد البيانات من وقت لآخر للتطورات المتلاحقة في مجال تكنولوجيا المعلومات قد يمثل خطرًا على الوثائق والمعلومات الإلكترونية، الأمر الذي تحتاج إلى تأمينها وحمايتها(**International Records Council on Archives , 2009**)

ويمكن تعريف أمن وحماية الوثائق في ضوء القيود وتحديد صلاحية الاستخدام بأنه "تلك المهام المعنية بحماية الوثائق والملفات والنظم من الوصول غير المصرح به و/ أو الأضرار أو الخسائر الناجمة عن الحريق والمياه والسرقة والتشويه غير المصرح به أو تحويرها أو تدميرها. (**Dickman J, Josph C., Charles,2002, p.6**) .وهي "فرض ضوابط على سبل وأساليب الوصول بهدف إضفاء الشرعية على حدود وصلاحية استخدام الوثائق (**فهد بن ناصر العبود, 2005,ص 152**).

وكذلك يمكن تعريف أمن وحماية الوثائق الإلكترونية من منطلق توفير الحماية للأجزاء المادية وغير المادية بأنها السياسات والممارسات والتقنية التي يجب أن تكون داخل المنظمة لتداول المعلومات الكترونيا عبر الشبكات بدرجة معقولة من الأمان، هذا الأمان ينطبق على الأنشطة والتخزين الالكتروني (**Robinson, Stephen and Linda Volonino, 2004, p.1**)

معايير أمن وحماية الوثائق والمعلومات

1. **معايير الأيزو:ISO standards** ويعد أشهر المعايير التابعة لها والمتعلقة بباقي المعلومات منها:

أيزو 27002: هذا المعيار يتضمن بعض السياسات والتوجيهات منها:

- السياسات الأمنية Security Policy. تنظيم أمن المعلومات أمن الموارد البشرية.
- الأمن البيئي والمادي الاتصالات وإدارة العمليات. التحكم في الوصول.
- اقتناء نظم وتطويرها وصيانتها إدارة الحوادث الأمنية للمعلومات.

أيزو 27001: هذا المعيار يقدم نموذج دوري يعرف (PDCAI) وهو يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المنظمة وعادة ما ينطبق على جميع أنواع المنظمات بما في ذلك المؤسسات التجارية والوكالات الحكومية وغيرها، ويتم هذا النموذج في أربع مراحل متتابعة هي: **(فهد فايز المدرع,2009,ص ص3-5)** :

1-الخطة: تأسيس نظام لإدارة أمن المعلومات. التنفيذ:
2-البدء في تنفيذ الخطط وتشغيلها.
3-التحقق: مراجعة النظام بعد تنفيذه. العمل.
4-صيانة وتحسين النظام.

أيزو 15408: يساعد هذا المعيار على التقييم والتحقق والتصديق على الضمانات الأمنية للمنتجات التكنولوجية، وكذلك يمكن تقييم الأجهزة والبرمجيات لمكافحة تغير المناخ في مختبرات معتمدة للتصديق.

أيزو 13335: ويتكون من سلسلة من المبادئ والتوجيهات وهي:

- أيزو 13335-1: عبارة عن توثيق للمفاهيم والنماذج لإدارة أمن التكنولوجيا المعلومات
- أيزو 13335-2: عبارة عن توثيق للتقنيات لإدارة أمن تكنولوجيا المعلومات.
- أيزو 13335-3: يشمل اختيار الضمانات كالضوابط الأمنية التقنية.
- أيزو13335-4: يشمل على التوجيه الإداري لأمن الشبكات. **(فهد فايز المدرع,2009,ص ص3-5)**

كما نص معيار الايزو رقم 15489 الجزء الثاني ان السجلات التي تتخذ الشكل الإلكتروني يمكن تدميرها من خلال إعادة صياغتها او اعادة كتابتها خاصة اذا لم يوجد ضمان لحمايتها من العبث في محتوياتها , لذا فإن التدمير المادي لوسائط التخزين هو الحل الافضل للتخلص من المعلومات افضل من إعادة تهيئة وسائط التخزين.(David T. Shaw , 2006)

المخاطر التي تهدد أمن وحماية الوثيقة الإلكترونية:

تتمثل أهم المخاطر التي قد تهدد أمن وحماية الوثيقة الإلكترونية في البنود الآتية:

- الوصول غير المرخص إلى الأجهزة ووسائط التخزين وكذلك إلى قواعد البيانات التي تعمل على تشغيل النظام سواء داخل أو خارج المنظمة.

- عدم كفاية إجراءات أمن وحماية الوثائق وكذلك قواعد البيانات كأن تكون غير محمية بشكل كافي أو يكون من السهل على الغير اكتشاف آلية الحماية المستخدمة فيه والقدرة على تعطيله.
- تعطل الآلات والتجهيزات وتوقفها عن العمل بسبب أي عطل ميكانيكي أو بسبب عطل في البرمجيات المستخدمة.
- التلف الذي يصاحب دخول الفيروسات أثناء انتقال المعلومات عبر قنوات أو وسائل الاتصال المختلفة.
- وجود بعض التجهيزات أو المحطات الطرفية في أماكن غير آمنه مما يجعل سرقة المعلومات أو البيانات أمرا سهلا **(أحمد حلمي جمعة، عصام فهد العربي ,2003,ص346)**

ويمكن تصنيف أهم المخاطر التي يمكن أن تهدد أمن وسلامة الوثيقة الإلكترونية في الآتي:

أولا/ من حيث المصدر:

1- المخاطر الداخلية:

يعد الموظفين بالمنظمة هم المصدر الرئيسي للمخاطر الداخلية التي يمكن أن تتعرض لها الوثيقة الإلكترونية وذلك لأن موظفي المنظمة على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنظمة وكذلك معرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، لذلك فإن موظفي المنظمة غير الأمناء يستطيعون الوصول للوثائق وإمكانية تدميرها أو تخريبها أو تغييرها. **(أحمد حلمي جمعة، عصام فهد العربيد،2003, 347)**، وهذه الأخطار يمكن أن تحدث أثناء إعداد وتصميم التجهيزات وقنوات الاتصال وأجهزة الحاسب التي ستعمل على تنفيذ النظم وذلك من خلال عمليات البرمجة أو تجميع البيانات أو إدخالها ومعالجتها واستخراج النتائج أو في تحديد الصلاحيات، ويمكن إيجاز تلك التهديدات في الآتي:

- العاملين في المنظمة الذين يطلعون على وثائق معينة غير مصرح لهم بالاطلاع عليها لاستخدامها في تحقيق مصالح معينة.
- ترتيب المعلومات عن طريق مستخدمو النظام ومن لهم حق الاطلاع على الوثائق سواء بقصد أو غير قصد. **(أحمد حلمي جمعة، عصام فهد العربيد , 2003,ص 348)**

2- المخاطر الخارجية External risks

وهي تلك التهديدات التي تأتي من خارج المنظمة من قبل أشخاص ليس لهم علاقة بها مثل قراصنة المعلومات أو المنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنظمة وتكمن خطورة تلك التهديدات في عدم معرفة المخترق ومدى اخترقه للنظام وحدود قدرته في التخريب وهدفه من وراء ذلك.

وتتمثل أهمية تلك التهديدات في الآتي:

- تهديدات الأجهزة Threats devices: وتشمل سرقة الأجهزة أو العبث بها أو تدميرها أو قطع الكابلات وأخيرًا تعرضها للتلف من خلال الحرائق أو المياه أو الطاقة الكهربائية.
- تهديدات المعلومات Information threats: وتشمل الحذف أو المسح أو التشويه الناتج عن مشاكل الأجهزة والبرامج والسرقة.

ثانيا/ تقسيم المخاطر من حيث المنسبب فيها:

1-مخـــاطر ناتجـــة عن العنصر البشـــري.

2- مخاطر ناتجة عن العنصر غير البشري.

1- مخاطر ناتجة عن العنصر البشري

والمقصود بها المخاطر والتهديدات الناتجة عن بعض التصرفات البشرية غير المتعمدة كالخطأ أو السهو والأخطاء المتعمدة وهي الأخطاء المتعلقة بالغش والتلاعب وتُشكل الأخطاء البشرية الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة الوثائق. (أحمد حلمى جمعة,2003,ص349)

2- مخاطر ناتجة عن العنصر غير البشري

وهذه المخاطر تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه. **(أحمد أبو موسى,2004, ص4-5)**

ثالثا / من حيث النعمد:

1-مخاطر ناتجة عن تصرفات متعمدة (مقصودة)

2-مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة)

أ-مخاطر ناتجة عن تصرفات متعمدة (مقصودة)

وتتمثل تلك المخاطر في تصرفات يقوم بها الشخص متعمدًا مثل إدخال بيانات خاطئة وهو يهمل ذلك أو قيامه بتدمير بعض البيانات متعمدًا، ذلك بهدف الغش أو التلاعب أو السرقة وتُعد هذه المخاطر بمثابة تحديًا كبيرًا لما تسببه من خسارة كبيرة ويمكن أن تتم هذه الجرائم الإلكترونية من

أشخاص داخل المنظمة أو من قبل أشخاص من خارج المنظمة يقومون باختراق نظم المعلومات بقصد تخريب وتدمير المعلومات. **(أحمد حلمى جمعة وآخرون , 2003,ص349).**

ب. مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة)

ويُقصد بتلك المخاطر تلك الأفعال التي تؤدي إلى تسرب معلومات إلى جهات غير ذات صلاحية أو فقد أو مسح معلومات مهمة أو تغيير في معلومات أو غير ذلك من مشاكل أمن المعلومات تكون في الغالب نتيجة الجهل وعدم الخبرة الكافية كإدخالهم بيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق إدخالها أو السهو في عملية التسجيل وكذلك إرسال تقارير بالخطأ غير المقصود أو وضع كلمة السر في مكان يسهل المعرفة به. **أحمد أبو موسى,2004,ص7).**

رابعا/ المخاطر من حيث علاقتها بمراحل النظام:

1-مخاطر المدخلات 2-مخاطر تشغيل البيانات 3-مخاطر المخرجات.

1-مخاطر المدخلات: وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال وذلك من خلال خلق بيانات غير سليمة أو تعريف بيانات المدخلات أو حذف بعض المدخلات أو إدخال البيانات أكثر من مرة. **(أحمد أبو موسى,2004,ص7)** ,وتتمثل المخاطر المتعلقة بأمن المدخلات في الآتي:

- الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
- الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
- التدمير غير المتعمّد للبيانات بواسطة الموظفين.
- التدمير المتعمّد (المقصود) للبيانات بواسطة الموظفين.

2-مخاطر تشغيل البيانات Processing

ويُقصد بها المخاطر المتعلقة بعملية التشغيل ومعالجة البيانات وهي تتمثل في الآتي:

- المرور (الوصول) غير الشرعي (غير المرخّص به) للبيانات والنظام .
- اشتراك العديد من الموظفين في كلمة السر.
- اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.
- إدخال فيروس الحاسب للنظام والتأثير على عملية تشغيل بيانات النظام.

3-مخاطر المخرجات Output:

ويُقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية التشغيل ومعالجة البيانات ويمكن أن يحدث ذلك من خلال الآتي:

- طمس أو تدمير بنود معينة من المخرجات. - خلق مخرجات زائفة وغير صحيحة.
- سرقة المخرجات أو إساءة استخدامها. - النسخ غير المصرح به من المخرجات.
- الكشف غير المسموح للبيانات عن طريق عرضها على شاشة العرض.
- توزيع المعلومات بواسطة أشخاص غير مصرّح لهم بذلك.
- توجيه المعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات.
- تسليم المعلومات لأشخاص لا تتوافر لديهم الناحية الأمنية. **(جمعة أحمد، العربيد,2003,ص36-38).**

أما عن الخطوات التي ينبغي على المنظمات تطبيقها؛ لضمان حماية الوثائق الإلكترونية، فهي كالتالي:

1. عمل نسخ احتياطية من الوثائق الإلكترونية ذات القيمة الدائمة.
2. نقل الوثائق الإلكترونية ذات القيمة الدائمة على الأرشيف فور انتهاء الحاجة إليها.
3. وضع نظام لتشفير نظم الحفظ، وكذلك وضع كلمات مرور Password.
4. ضبط بيئة الأجهزة ووسائط التخزين وفي ظروف تحميها من الرطوبة والأتربة ... إلخ من العوامل التي قد تؤثر سلبًا على أجهزة ووسائط التخزين، وبالتالي قد يؤثر أيضًا بالسلب على تلف الوثائق المخزنة بها.
5. استخدام نظم أمن ذات تقنية عالية، بما يضمن منع الوصول غير المصرح به للوثائق المخزنة على الأجهزة ووسائط التخزين.
6. في حالة وجود وثائق لا يمكن استعادتها مرة أخرى في حالة فقدها أو تلفها، ينبغي تخزينها في أماكن مستقلة عن نظم الحفظ المستخدمة (Dickman J, Josph C., Charles,2002)
7. التحقق من هوية المستخدم وإجراءات الوصول والتي ينبغي أن تكون موثقة.
8. دليل على تتضمن قوائم المستخدمين الحاليين والسابقين كلمات السر والامتيازات والمسئوليات.
9. وظائف المستخدمين وتقييد الوصول إلى تلك الوثائق اللازمة للمستخدمين
10. نظام الوثائق ينبغي أيضًا أن يشمل السياسة المتعلقة بإنشاء وصيانة وحماية الوثائق، على أن يتم ذلك من خلال الإجابة على الأسئلة مثل: من المصرح له بتعديل البيانات؟ متى؟ كيف؟ - من مصرح له بحذف البيانات؟

الطرق والإجراءات اللازمة لحماية المعلومات والوثائق:

(1) حماية المعلومات الحكومية على مستوى الأنظمة والبرامج:

لا شك أن برامج وأنظمة الحاسب الآلي المستخدمة في أية منظمة تكون دائمًا عرضة للتهديد من قِبَل أشخاص غير مصرّح لهم لمحاولة التدمير أو التغيير ومحاولة الحصول على نسخ منها. لذا فإنه يجب التركيز على حماية هذه البرامج والأنظمة وإبعاد أي خطر قد يهدد أمنها وسلامتها ومن أهم الإجراءات التي تساعد على ذلك ضرورة تحديد الأشخاص المصرّح لهم بالاطلاع على برامج وأنظمة الحاسب داخل المنظمة، كما يجب الاحتفاظ بنسخة احتياطية للبرامج والأنظمة والبيانات في مكان آمن خراج المنظمة مع ضرورة تحديث البيانات بصفة دورية.

ويُفضل تسجيل الأخطاء والمخالفات التي تحدث ومراجعتها لتفادي حدوثها مستقبلاً وأن يتم اختيار كلمات السر والأرقام الرمزية المستخدمة للعمل على النهايات الطرفية أو للدخول لمبنى المنظمة وغرف الحاسب الآلي وغرفة السجلات والوثائق فيها بشكل عشوائي مع ضرورة تغييرها بشكل دوري وأن يتم تسليمها لصاحبها بطريقة سرية جدًا مع ضرورة قيام إدارة المنظمة بالاستفادة من التقدم التكنولوجي في مجال تخزين المعلومات حيث تتوافر الآن وسائل ذات قدرة عالية على التخزين لمعلومات هائلة على أشرطة صغيرة مثل أقراص الليزر والأقراص الضوئية.

وتشتمل برامج وأنظمة الحاسب الآلي في المنظمة على النظام الذي يُتّبع تحديد مستخدم النهاية الطرفية ووقت الاستخدام ووقت الانتهاء من الاستخدام على أن يتم كل ذلك والاحتفاظ به للرجوع إليه عند الضرورة. كما يجب على إدارة المنظمة القيام وبصورة مفاجئة على فترات بمراجعة جميع العمليات التي تتم داخل المنظمة مع ضرورة إجراء الرقابة الداخلية على جميع الإجراءات المطبقة داخل المنظمة. **(هشام محمد فريد رستم,1996, ص92).**

(2) حماية المعلومات على مستوى الأفراد العاملين على النظام:

يشكل الأفراد العاملون عل النظام الآلي في المنظمة أحد التهديدات القوية التي يمكن أن تؤثر على أمن وسلامة المعلومات. فقد يرتكب الفرد خطأ عند استخدام النظام أو أثناء إعداد وتجهيز البرامج مما يقلل من فأعليتها كما يجب عدم إغفال نقطة مهمة وهي أنه من المحتمل أن يكون أحد الأفراد العاملين على النظام ليس فوق مستوى الشبهات فيصبح من أكبر التهديدات على النظام وما يحتويه من برامج وأنظمة وبيانات. لذا فإن من أهم الإجراءات التي يمكن أن تساعد المنظمات على حماية المعلومات من تهديد بعض العاملين لديها ما يلى: **(هشام محمد فريد رستم,1996, ص93):**

1. التحري الدقيق عن كل شخص يتقدم لوظيفة ترتبط بإدارات الحاسب الآلي في المنظمة وخاصة المبرمجين.
2. الحرص على توظيف المؤهلين علميًا وعمليًا ما أمكن لتقليل احتمال الوقوع في الخطأ أثناء العمل.
3. إعطاء الأفراد العاملين على النظام وخاصة الجدد منهم دورات تدريبية وتعليمية تتعلق بأمن وسلامة المعلومات.
4. ضرورة إصدار النشرات الدورية المتعلقة بالنواحي الأمنية والتأكد من أن كل موظف لديه الخلفية الأمنية والقدرة على مواجهة أي تهديد لأمن وسلامة المعلومات.
5. يُفضل أن تقوم المنظمة بالاشتراك بالدوريات التي تنشر وتتعلق بأمن وسلامة المعلومات ليطلع موظفي المنظمة على كل جديد في أمن وسلامة المعلومات.
6. إخضاع المبرمجين ومحللي النظم وبصفة مستمرة للمراقبة من قِبَل مشرف صاحب خبرة طويلة في هذا المجال وإشعارهم بأنهم خاضعون للرقابة الأمنية المستمرة من قِبَل إدارة المنظمة.
7. إبعاد أي فرد من العاملين يمكن أن يهدد أمن وسلامة المعلومات كما يجب أن توقع الإدارة عقوبات رادعة عليهم.
8. عند انتهاء أو إنهاء خدمات أحد الموظفين العاملين على النظام فيجب إبعاده عن المواقع الحساسة في المنظمة مع ضرورة قيامه بتسليم جميع ما يحتفظ به من مفاتيح أو بطاقات ممغنطة للدخول والخروج من وإلى المنظمة كما يجب على إدارة المنظمة أن تقوم بإلغاء جميع الأرقام والرموز السرية الخاصة به.
9. أخذ التعهد على الموظف المنتهي خدماته في المنظمة بالمحافظة على أسرار العمل التي كان يطلع عليها، وخاصة البرامج والأنظمة.

(3) <u>الوسائل التقنية لحماية المعلومات</u>:

هناك العديد من وسائل الحماية التقنية للمعلومات والحماية التقنية تعني استخدام الأجهزة والتقنيات المتطورة التي تمنع محاولات الدخول غير المشروع وتحد منها بقدر الإمكان كبرامج الجدران النارية والبطاقات الممغنطة وبرامج مكافحة الفيروسات وتنحصر أهم الوسائل التقنية لحماية المعلومات فيما يلي:

1/3 برامج الجدران النارية: Firewalls

برمج تقوم على عزل الشبكة المحلية عن الشبكات الخارجية جزئيًا أو كليًا وقد تكون الجدران النارية تقع بين الشبكة المحلية والشبكة العالمية لحماية معلومات الشبكة المحلية والتحكم في عمليات الدخول إليها. **(طارق بن عبدالله الشدي, 1416, ص 139) .**

وبرامج الجدران النارية أو جدران الحماية كما يطلق عليها عبارة عن مرشحات تتبع صلاحية وحدود الاستخدام للمصرّح لهم فقط واستخدام النظام وبالرغم من أنها تعطل انتقال البيانات نسبيًا إلا أنها ذات فاعلية في منع محاولات الاختراق والتعدي. **(محمد دباس الحميد,2003,ص42).**

- حماية وتأمين البيانات الموجودة على الأجهزة.
- تقوم بتشفير البيانات عند إرسالها عبر الشبكات فقط.
- توفير الاحتياطات اللازمة لحماية البيانات المستخدمين المخزنة في أجهزتهم.

2/3 الكاشفات الإلكترونية والبيولوجية:

هي أجهزة تقنية متطورة تعتمد على خصائص البيولوجية حيث تقوم بقياس السمات الإنسانية وتطابقها مع تلك المسجلة بذاكرة الحاسب الآلي لكي تحدد صلاحية وحدود الاستخدام والدخول على النظام وهي بجانب توفيرها الحماية التقنية يمكن استخدامها في توفير الحماية المادية بمنع فتح الأبواب لغير المصرّح لهم.

ومن أهم هذه التقنيات: تقنية الكشف عن ملامح الوجه، تقنية الكشف عن قزحة العين ،تقنية التعرف على الصوت ،تقنية الكشف بصمة الأصبع ،تقنية الكشف عن كف اليد.

4/3برامج مكافحة الفيروسات: Antivirus

يُستخدم مصطلح الفيروس ليُشير إلى بعض البرامج المصممة للإضرار بأجهزة الحاسب الآلي فهذه البرامج تبدو مثل الألعاب ولكنها في الحقيقة تقوم بتهيئة الأقراص الصلبة وتمسح جميع البيانات الموجودة فوقها وتنتقل الفيروسات من جهاز لآخر عن طريق الأقراص والفلاش في الغالب ويمكن أن تنتقل الفيروسات عبر كابل الشبكات لذلك قد تتعرض أجهزة الحاسب الآلي المرتبطة بالشبكات لهجوم الفيروسات بصفة مستمرة. **(محمد دباس الحميد، ,2004,ص54)**

ولم يقف العلم عاجزًا أمام الفيروسات فتم ابتكار برمج لمكافحة الفيروسات وإزالتها من النظام أول بأول حيث تقوم بمنع دخول الفيروسات على النظام واكتشافها قبل حدوث الضرر والقضاء عليها عند اكتشافها فضلاً عن تحديثات نفسها بشكل تلقائي عن طريق الإنترنت لزيادة قدرتها وكفاءتها على مكافحة الفيروسات الجديدة. وتقوم برامج مكافحة الفيروسات باستخدام تقنية البحث عن الفيروسات من خلال تفحص السلوك ومراقبة جميع الملفات الموجودة على الجهاز برصد أي تغيير

يحدث من خلال تقنية اختيار لتكامل ببناء سجل يتضمن أسماء جميع الملفات الموجود على الحاسب وحجمها وتاريخها ومتابعة أي تغيير أو نشاط غريب عليها. **(عاصم يس محمد, 2001,ص149).**

4/3 التشفير والإخفاء: Encryption and Concealment:

يُقصد بتشفير المعلومات تحويلها إلى رموز غير مفهومة وغير ذات معنى لمنع غير المرخّص لهم من فهمها حتى عند الاطلاع عليها. **(عاصم يس محمد, 2001,ص149).**

فعملية التشفير تتضمن تحويل النصوص العادية إلى نصوص مشفره أما الإخفاء فهو وضع المعلومات المتبادلة داخل صورة ثابتة أو متحركة بحيث لا يمكن رؤيتها أو ملاحظتها إلا لمن لديه معلومة عنها. ويُعد التشفير أحد وسائل حفظ معلومات المنظمة من خلال تغيير مظهرها لإخفاء معناها الحقيقي بعدة طرق فتظهر كلمات غريبة مبهمة. وطريقة فك الشفرة هي عكس الإجراءات التي تستخدم في التشفير. ويُعد التشفير وإخفاء المعلومات من الوسائل المهمة لضمان أمن المعلومات حيث يستخدمان للتغلب على عدد كبير من الأخطار **(Farmer, Jackie , 2006,p.168) .**

5/3 أدوات كشف الاختراقات:

تضاف أدوات صداً ومنع الاختراقات إلى مستويات الحماية التي يجب توفيرها للنظم، وتعتبر هذه الإضافات بمثابة حماية مبكرة للنظام ولكن فيما لو تمكن مهاجم أو برنامج محدد من إحداث خلل بالنظام فإن أدوات أخرى يجب استخدامها تسمى أدوات الكشف عن الاختراقات ويجب أن يتم فحص هذه الوسائل من فترة لفترة حتى يتمكن النظام من العمل بفعالية، كما أنها تفيد مسئولي النظم في توظيف التقارير التي تنتجها النظم آلياً فيوضع إحصائيًات محددة ووضع تصورات حول أنشطة النظام وأمنه وتختلف عن الجدران النارية بأنها تحتاج إدارة ومتابعة أكبر من قبل مراقب ينظم المعلومات والقائمين على تتبع أمن نظم المعلومات[3].

6/3أمن الشبكات: Network Security

يتم في أغلب الحالات نقل البيانات عن طريق الشيكات لذلك يجب الاهتمام بأمنها وحمايتها؛ لضمان سرية وسلامة المعلومات ووصولها إلى الجهات المعنية، ويتحقق أمن الشبكات من خلال اتخاذ إجراءات الحماية اللازمة التي تنقسم حسب طبيعة المخاطر التي تتعرض لها إلى قسمين هما:

1/6/3 إجراءات الحماية المادية:

يتضمن إجراء التوصيلات والتمديدات بين الأجهزة وبشكل آمن من خلال تمريرها عبر قنوات غير مكشوفة يصعب الوصول إليها وعزل الكابلات داخل أنابيب بلاستيكية مع وضع أجهزة استشعار لإطلاق إنذار عند الخطر.

2/6/3 إجراءات الحماية غير المادية:

- عنونة الشبكات يجب الالتزام بوضع عناوين لجميع الأجهزة المرتبطة بالشبكة؛ لكي يمكن التعرف عليها عند تشغيلها، ومن ثم حماية جميع العناوين والأجهزة التي تقوم بترجمة وتحويل العناوين من الأشخاص غير المصرح لهم بالتعامل معها.
- متابعة جميع محاولات الدخول على النظام سواء الصحيحة أو الفاشلة.
- توفير آليات الحماية بعد الدخول على النظام كالتزام المستخدم بالخروج من النظام عند عدم استخدامه، والخروج الآلي عند عدم استخدام النظام لفترة معينه والخروج من النظام عند عدم استخدام النظام لفترة معينة والخروج من النظام عند نهاية العمل الرسمي.
- تشفير البيانات عند إرسالها عبر الشبكة؛ لضمان عدم تحويرها أو الاطلاع عليها أو العبث بها.
- اتخاذ إجراءات مراجعة الشبكة بعد تشغيلها والإشراف عليها من قبل إداريين وفنيين؛ بهدف اكتشاف وتحسين خدماتها باستمرار. .(**محمد دباس الحميد، ,2004,ص54).**

7/3 توفير نظام احتياطي: Back-up System

نتيجة لما قد تحدثه الكوارث من آثار سيئة على المنظمات وخصوصًا إدارات الحاسب والتي قد تصل إلى حد التدمير الشامل فإنه لابد من توفير نظام احتياطي للنظام داخل المنظمة حتى يمكن تفادي أية عملية توقف للنظام قد تحدث بسبب هذه الكوارث. .(محمد دباس الحميد، ,2004,ص54).

ويُقصد بالنظام الاحتياطي مجموعة الإجراءات والأجهزة والمعلومات والبرامج والأشخاص التي يجب توفيرها في أماكن ما خارج المقر الرئيسي للمنظمة وذلك لاستخدامها في حالة حدوث ما يمنع استخدام النظام القائم (الأساسي) سواء كان ذلك بسبب عرضي أو متعمّد. ولاستمرار أداء وفاعلية النظام الاحتياطي فإنه لابد من وضع إجراءات كفيلة بصيانة هذا النظام والمحافظة عليه والتأكد من سلامته بصفة مستمرة. ويُفضل أن يكون عمل هذا النظام آليًا بحيث يعمل مباشرة عند تعطل النظام الأساسي وذلك لحماية عدم انقطاع الخدمة التي تقدم للمستفيدين ويجب أن يتم إجراء تجارب التحويل بين النظامين بصفة دورية لضمان حسن الأداء وعلى الرغم من أهمية وجود مثل هذا النظام لكل منظمة إلا أن ارتفاع التكاليف لتأسيس مثل هذا النظام قد لا يتيح لبعض المنظمات توفير هذا النظام وذلك لعدم قدرتها على تحمل تكاليفه المادية إلا أن هناك بعض الخيارات التي يمكن أن تؤدي نفس الغرض مع التباين في تكاليف الإنشاء ومنها:

1/7/3نظام احتياطي كامل: من البديهي أن يكون هذا النظام ذا تكلفة عالية لما يتطلبه من جهود وتجهيزات كثيرة تماثل النظام الأساسي من حيث الأجهزة والأيدي العاملة إلا أن ذلك لا يُقارن بماتحتويه هذه الأنظمة من معلومات مهمة وحساسة لا تحتمل أي انقطاع. (**منير محمد الجنبيهي، ممدوح محمد الجنبيهي ,2007, ص79-87)** .

2/7/3 مركز فرعي: أي أن يكون أحد فروع المنظمة مركزًا احتياطيًا للنظام الأساسي بحيث يزود ببعض الأجهزة كوسائط التخزين ويتم ربطه بالشبكة الرئيسية للمنظمة واستخدامه بديل للمركز الرئيسي في حالة حدوث أي طارئ.

3/7/3الاتفاق المتبادل: أي أن يتم اتفاق منظمتين لديهما أنظمة مماثلة على أن يكون نظام كل منظمة احتياطيًا للمنظمة الأخرى ليتم استخدامه عند حدوث أي طارئ ويُلاحظ أن هذا الخيار هو أقل الخيارات تكلفة مالية.

وتُعد من أهم الإجراءات الإدارية الوقائية التي يجب اتخاذها على هذا النظام من قبل إدارة المنظمة ما يلي:

- يجب تطبيق جميع إجراءات الحماية المتخذة في المركز الرئيسي على النظام الاحتياطي.
- يجب أن يكون مقر النظام الاحتياطي غير معروف إلا لدى الأشخاص المعنيين فقط.
- يجب أن يوضع مركز النظام الاحتياطي في مكان بعيد عن المقر الرئيسي للمنظمة.
- إجراء الصيانة الدائمة لكافة متعلقات النظام الاحتياطي لضمان استمرارية الأداء.
- القيام بإجراء عمليات تحويل النظام من الأساس إلى النظام الاحتياطي خلال فترات ليست بعيدة وذلك للتأكد من صلاحية النظام الاحتياطي. (محمد إبراهيم أبو معطي ,2009,ص 91).

سياسة أمن المعلومات الحكومية على بوابة إمارة أبو ظبي الالكترونية

أولا/ التعريف بحكومة ابو ظبي الالكترونية[1]:

تتولى حكومة الإمارات الإلكترونية مهمة صياغة استراتيجية الحكومة الإلكترونية على المستوى الاتحادي في دولة الإمارات والإشراف على تنفيذها، وكذلك تعزيز البنية التحتية المشتركة للجهات الحكومية الاتحادية. كما تعمل على رفع جاهزية التحول الالكتروني للخدمات التي تقدمها الحكومة الاتحادية، بما يضمن توفير خدمات حكومية متطورة وفعالة، يمكن الحصول عليها بسهولة وعلى مدار الساعة.

---

[1] لمزيد من المعلومات حول الحكومة الالكترونية بأبو ظبى يتم الرجوع بوابة الحكومة على شبكة الويب وهو https://www.abudhabi.ae/portal/public/ar/homepage?_adf.ctrl-state=1d6g561hpk_4&_afrLoop=6964139499380832

وتشرف حكومة الإمارات الإلكترونية على البوابة الرسمية الاتحادية لحكومة دولة الإمارات العربية المتحدة، وهي البوابة التي تضم كافة الخدمات والمعلومات الحكومية الاتحادية والمحلية في الدولة بهدف توفير وقت وجهد ومال المستخدمين.

وقد قام فريق حكومة الإمارات الإلكترونية بصياغة عدد من الأدلة والإرشادات التوجيهية استناداً إلى أفضل الممارسات العالمية. وتوفّر هذه الوثائق إضاءات تستهدي بها الجهات الحكومية في سعيها لتعزيز حضورها الإلكتروني على شبكة الإنترنت. وتتناول تلك الأدلة الإرشادية المحتوى الإلكتروني، والمشاركة الإلكترونية، ومواصفات البيانات المفتوحة، واستخدام أدوات التواصل الاجتماعي.

أهداف حكومة أبوظبى الإلكترونية:

1. تدعم الحكومة الإلكترونية عمليات الحكومة الكلاسيكية من حيث تقديم الخدمات آلياً لجمهور المستفيدين ومشاركتهم في صنع القرار وصولاً إلى تحقيق شفافية أكثر في عملية الحكم
2. كما تهدف إلى تخفيف الأعباء المالية في الإدارات العامة لجهة كلفة إجراء الخدمات مع المحافظة على مستويات عالية لجودة الخدمات.
3. خدمة المواطنين والشركات والمستثمرين
4. توصيل الخدمة إلى طالبها.
5. - سرعة إنجاز الخدمات والاعمال الادارية.
6. التميز ورفع كفاءة العمل وتحديث نظم العمل بالوزارات والهيئات
7. توفير مناخ مشجع للمستثمرين وتذليل العقبات التي يوجهونها والتي تتمثل بشكل أساسي في بطء الإجراءات وتعقيدها، مما سينعكس بشكل إيجابي على تشجيع الاستثمار المحلي وجذب المزيد من الاستثمارات الأجنبية.[1]
8. تهيئة الجهاز الحكومي للاندماج في النظام العالمي: وتقوم الحكومة الإلكترونية بالمساعدة في ذلك عن طريق تدعيم الجهاز الحكومي بأحدث أساليب الميكنة

---

(1) لمزيد من المعلومات حول الحكومة الالكترونية بأبو ظبى يتم الرجوع بوابة الحكومة على شبكة الويب وهو https://www.abudhabi.ae/portal/public/ar/homepage?_adf.ctrl-state=1d6g561hpk_4&_afrLoop=6964139499380832

ثانيا/ سياسة أمن المعلومات على حكومة أبو ظبي الإلكترونية:

فيما يتعلق بسياسة أمن وحماية المعلومات على بوابة حكومة ابو ظبي الالكترونية فقد قام مركز أبو ظبي للأنظمة الإلكترونية والمعلومات بتطوير عدة مبادرات وبرامج ومنشورات من أهمّها:

- سياسة أمن المعلومات: وضع البرنامج توجّهاً شاملاً لبرنامج حكومة أبو ظبي لأمن المعلومات
- معايير أمن المعلومات: يهدف إلى توحيد معايير وضوابط أمن المعلومات.
- دليل السياسات والإجراءات: عبارة عن سلسلة من الإرشادات الإجرائية والفنية للجهات الحكوميّة.
- برنامج المعرفة الإلكترونية: هدفه تحديد الفجوات الرقميّة وتحسين قدرات تكنولوجيا المعلومات والاتصالات لجميع شرائح المجتمع في أبو ظبي من خلال مبادرات محددة وهادفة.

وقد قامت هيئة تنظيم الاتصالات وهي الجهة المسؤولة عن إدارة كافة نواحي صناعة الاتصالات وتكنولوجيا المعلومات في دولة الإمارات بإنشاء مركز الاستجابة لطوارئ الحاسب الآلي في عام 2008 كمركز تنسيق أمن المعلومات في دولة الإمارات. ويهدف المركز إلى تحسين معايير وممارسات أمن المعلومات وحماية البنية التحتية لتكنولوجيا المعلومات بالدولة، فضلاً عن تسهيل الكشف عن مخاطر واختراقات الإنترنت ومنع حدوثها وتوفير الاستجابة الضرورية لها.

وتعمل حكومة ابو ظبى على القيام بتأمين المعلومات الحكومية بشكل يكفل مواجهة المخاطر ويتناسب مع حجم الضرر الذى قد ينجم عن فقدان مثل تلك المعلومات أو إساءة استخدامها او الحصول عليها أو تعديلها بطريقة غير قانونية , وتحقيقا لهذا الغرض , قامت حكومة أبو ظبى بوضع سياسة لأمن المعلومات بشكل يكفل السرية وصحة المعلومات والاتاحة الملائمة لجميع المعلومات .

وتعتبر ادارة المخاطر والرقابة الأمنية أساسا لبرنامج أمن المعلومات والذي يتطلب أن تقوم الجهات الحكومية بتأمين المعلومات الحكومية بشكل يكفل مواجهة المخاطر ويتناسب مع حجم الضرر الذي قد ينجم عن فقدان تلك المعلومات أو اساءة استخدامها او الحصول عليها او تعديلها بطريقة غير قانونية. وهكذا تتطلب جميع المعلومات الحكومية مستوى معينا من الحماية، ولكن المعلومات الحساسة تحديدا تتطلب رقابة إدارية خاصة. ويتقرر تحديد الرقابة الأمنية الملائمة وإمكانية تطبيق الرقابات الادارية الخاصة من خلال تنفيذ عمليات ادارة المخاطر. (مركز أبو ظبي الالكترونى , 2008).

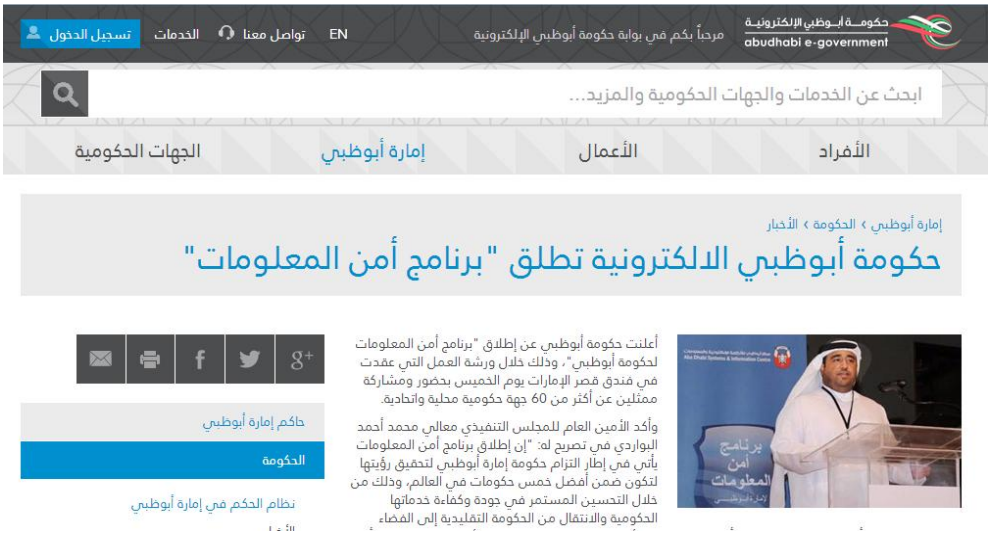
إدارات أمن المعلومات بحكومة أبو ظبي:

وقد قام مركز أبو ظبي الإلكتروني التابع والمسئول عن ادارة امن المعلومات على بوابة الحكومة الالكترونية بإنشاء عدد من الادارات تقوم كل منها بمتابعة سير المعلومات وضمان أمنها وحمايتها من أي اخطار قد تتعرض لها، وتتمثل هذه الادارات في(مركز أبو ظبي الإلكتروني , 2008).

أولا/إدارة المخاطر:

تنص سياسة إمارة أبو ظبي على ضرورة تنفيذ عملية إدارة المخاطر لأمن المعلومات على مستوى الحكومة أو الأفراد المصرح لهم بالدخول الى المعلومات او النظم الحساسة من أجل تحقيق ما يلي:

1. إخضاع كافة الخدمات الحكومية لتقييم المخاطر، والذي يجب من خلاله تحديد الرقابة الأمنية استنادا الى المخاطر، كما يجب تحديد إمكانية تطبيق مراقبة إدارية خاصة وتتضمن هذه المراقبة إعداد خطة أمن المعلومات.
2. إجراء اختبار أمن وتقييم الرقابات المفروضة على فترات متقاربة بحيث لا تقل عن مرة في السنة.
3. الحصول على الاعتماد والتصديق لجميع الخدمات الحكومية الملائمة والمحافظة عليها
4. تنفيذ إدارة المخاطر بصورة متواصلة على جميع الخدمات الحكومية.



شكل(1) يبين إطلاق حكومة أبو ظبي لبرنامج أمن المعلومات على بوابة الحكومة الالكترونية

ثانيا / أمن المرافق والبيئة المحيطة:

تتضمن سياسة امارة ابو ظبي على ضرورة تطبيق برنامج أمن المرافق والبيئة المحيطة على مستوى الحكومة، وعلى الجهات الحكومية والموظفين والمتعاقدين التي يجوز لها الدخول الى المعلومات او النظم الحساسة الالتزام بهذا البرنامج من اجل:

- ضمان حماية مرافق معالجة المعلمات الهامة والحساسة من الاختراق والاضرار والتدخل غير القانونى.
- حماية المعدات من التهديدات المادية والبيئية.

ثالثا/ إدارة الإتصالات والعمليات:

تتضمن مهام هذه الادارة في مجال أمن المعلومات ما يلي:

1- ضمان تحديد المسؤوليات والاجراءات لإدارة جميع مرافق معالجة المعلومات وتشغيلها.
2- اعداد الاحتياطات لمنع الشفرات التخريبية والشفرات المتنقلة غير القانونية.
3- عمل نسخ احتياطية من المعلومات وفحصها بانتظام.
4- الادارة الآمنة للشبكات.
5- ضبط الوسائط وحمايتها ماديا.
6- حماية الخدمات الحكومية الالكترونية بدرجة كافية.
7- مراقبة النظم والحوداث المتعلقة بأمن المعلومات.

رابعا / إدارة الهوية ووسائل الدخول:

تتضمن هذه الادارة المهام الآتية لحماية أمن المستندات الالكترونية من اجل: -

1- التحكم بالدخول الى المعلومات ومرافق معالجة المعلومات وإجراءات العمل.
2- ادارة الدخول المستخدمين.
3- تحديد مسئوليات المستخدمين والابلاغ عنها
4- مراقبة الدخول الى خدمات الشبكتبن الداخلية والخارجية
5- مراقبة الدخول الى نظم التشغيل.
6- مراقبة الدخول الى المعلومات المحفوظة في نظم التطبيقات.
7- تطبيق الحماية الملائمة عند استخدام اجهزة الحاسب المحمولة وخدمات العمل عن بعد .

خامسا/ إدارة حيازة نظم المعلومات والحفاظ عليها :

تتضمن مهام هذه الادارة ما يلي:

1- تحديد المتطلبات الامنية.
2- بناء رقابات أمنية ملائمة ضمن تصميم التطبيقات
3- اعداد سياسة المراقبة بنظام الشفرة وأساليب الشفرة المساندة للإدارة.
4- التحكم بالدخول الى ملفات النظام وشفرة المصدر.
5- ضمان الأمن في عمليات التطوير والمساندة.
6- ادارة الجوانب الفنية المعرضة للاختراق.

سادسا/ إدارة الحوادث العارضة:

تتضمن مهاما هذه الادارة المهام اللازمة لحماية أمن المستندات الالكترونية من اجل: -

1- ضمان الابلاغ عن الحوادث المتعلقة بأمن المعلومات ونقاط ضعفها في الوقت المناسب
2- تطبيق منهج دائم وفعال لإدارة الحوادث العارضة المتعلقة بأمن المعلومات بحيث يتضمن عملية التحسين المستمر.

وقد ألزمت سياسة إمارة أبو ظبي الجهات الحكومية بتعيين ضابط أول لأمن المعلومات يتولى قيادة برنامج أمن المعلومات في الجهة وادارته بما يضمن تطبيق سياسة امن المعلومات ومراقبة تنفيذها والالتزام بها. وتقوم الحكومة الالكترونية بإمارة أبو ظبي باستخدام إجراءات وضوابط مضادة لمخاطر تهديد المستندات على موقع البوابة وهي نوعين:

أ. <u>ضوابط إدارية:</u>

1- ضوابط التوجيه والتي عادة ما تكون ادارية، مثل وضع سياسات، والمطالبة بالعمل بمقتضى هذه السياسات.
2- الضوابط الوقائية التي تحمي نقاط الضعف وتجعل الهجوم فاشلاً أو تَحدُ من آثاره، وتحتاج الى الرقابة المستمرة لعناصر النظام.
3- ضوابط الكشف التي تؤدي لاكتشاف الهجمات.
4- الضوابط التصحيحية والتي تقلل من تأثير هجوم أوتمنعه.
5- ضوابط إعادة التهيئة والتي غالبا ما ترتبط مع استمرارية الأعمال والتعافي من الكوارث.

ب. ضوابط تعتمد على تقنيات الحاسب الآلي:

1. استخدام الصلاحيات وكلمات السر.
2. النسخ الاحتياطي Back up
3. تكامل البيانات Data Integrated .
4. التشفير Encryption
5. استخدام أنظمة RAID.
6. مضادات الفيروسات والرسائل المشبوهة Antivirus
7. الجدران النارية Firewall.
8. أنظمة المراقبة Control System

الإجراءات العامة لتامين وحماية المعلومات بامارة أبو0. ظبي:

وضعت هيئة الاتصالات بإمارة أبو ظبي مجموعة من الإرشادات لضمان أمن المعلومات الحكومية وهي:

- تثبيت برنامج مكافحة الفيروسات وتحديثه بشكل مستمر.
- عدم استخدام نفس اسم المستخدم وكلمة المرور على مواقع إلكترونية مختلف-
- عدم إدخال بيانات بطاقات الائتمان أو الحسابات البنكية في أي موقع دون التأكد من مدى الأمان الذي يتمتع به ذلك الموقع.
- إذا كنت تعمل لدى أية هيئة أو مؤسسة سواء أكانت حكوميةً أم خاصة، يجب التأكد من وجود اتفاقية عدم الكشف عن المعلومات والمعروفة باسم اتفاقية السرية، قبل تبادل أية معلومات مع طرف ثالث خارج مؤسّستك
- استخدام جهاز تمزيق الأوراق للتخلص من أية أوراق تحتوي على معلوماتك الشخصية -
- عدم الاستجابة لرسائل البريد الإلكتروني التي تطلب منك بيانات شخصية.
- مراجعة سياسة الخصوصية الخاصة بالمواقع الإلكترونية التي تنوي التسجيل بها أو تزويدها ببياناتك الشخصية
- التأكد من خصوصية كلمة المرور ويفضل أن تحتوي على مزيج من الأرقام والأحرف الكبيرة والصغيرة، وأن لا تقل عن 8 أحرف.

المصادر والمراجع:

أولا/ المراجع العربية:

1. أحمد حلمي جمعة، وآخرون. نظم المعلومات المحاسبية: مدخل تطبيقى معاصر.ـ عمان: دار المناهج للنشر والتوزيع، 2003، ص 346.
2. أحمد عبد السلام أبو موسى. مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المنشآت السعودية، مجلة كلية التجارة للبحوث العلمية، كلية التجارة – جامعة طنطا، ع2، 2004، ص 4، 5.
3. أحمد الكبيس. تطور النظم الآلية في المكتبات في الحوسبة إلى الرقمنة الافتراضية، مجلة النادي العربي للمعلومات، ع 3، 2008، ص ص 1: 4.
4. شريف كامل شاهين: مصادر المعلومات الإلكترونية في المكتبات ومراكز المعلومات. - القاهرة: الدار المصرية اللبنانية، 2000، ص 157، 158.
5. طاهر داود. الحاسبات وأمن المعلومات.ـ الرياض: معهد الإدارة العامة، 2001.
6. اصم يس محمد: أثر الثقافة على المنظور والعمل الأمني، مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من 21 – 24 ذو القعدة 1428، الموافق 1- 4 ديسمبر 2001، الرياض.
7. ثمان الصديق احمد محمد , المستند الالكتروني واهميته وضرورة اصدار تشريع يكفل حجيته ويضع ضوابط له , 2009, متاح على : www.carjj.org/sites/default/files/symp-rec-edoc-sudan.doc .
8. عمار كريم كاظم,نارمان جميل نعمة . القوة القانونية للمستندات الالكترونية , 2007 , متاح على : http://www.iasj.net/iasj?func=fulltext&aId=29533
9. عوض حجاج علي أحمد، عبد الأمير خلف حسين. أمنية المعلومات وتقنيات التشفير. ـ عمان: دار الحامد للنشر والتوزيع، 2005، ص ص 196، 197.
10. فهد فايز المدرع . المعايير العالمية لأمن المعلومات ،مركز التميز لأمن المعلومات ، 2009،متاح على:http://faculty.mu.edu.sa/public/uploads/1335577864.0351المعايير%20العالمية%20لأمن%20المغلومات.pdf
11. فهد بن ناصر العبود. الحكومة الإلكترونية بين التخطيط والتنفيذ، الرياض: مكتبة الملك فهد الوطنية، 2005، ص152.

12. قاسم أبو حرب. إشكاليات الحفظ الدائم للسجلات الأرشيفية الإلكترونية. الندوة السنوية للفرع الإقليمي للمجلس الدولي للأرشيف، 30 فبراير- القدس: المجلس الدولي للأرشيف، 2003، ص4.

13. محمد إبراهيم أبو معطي "التخطيط الوقائي ضد كوارث الحاسبات الآلية، المركز العربى للدرسات الأمنية والتدريب , الرياض , 1990 ص 91، 92.

14. محمد دباس الحميد، ماركو إبراهيم مينو. حماية أنظمة المعلومات. - عمان: دار الحامد للنشر والتوزيع، 2005، ص34

15. محمد بن عبدالله القاسم. سياسات أمن المعلومات- سلسلة إصدارات مركز البحوث والدراسات. - الرياض: كلية الملك فهد الأمنية، 2005، ص 34، 35.

16. محمد محمود مكاوي. البيئة الرقمية بين سلبيات الواقع وآمال المستقبل 34 (سبتمبر 2003)مركز أبو ظبى الالكترونى والمعلومات ،سياسة أمن المعلومات ،حكومة أبو ظبى ، 2008. متاح على :
https://www.abudhabi.ae/cs/groups/public/documents/publication/mtm1/mtiw/~edisp/adegp_nd_135120_ar.pdf

17. منير محمد الجنبيهي، ممدوح محمد الجنبيهي. أمن المعلومات الإلكترونية. - الإسكندرية: دار الفكر الجامعي، ص ص 79، 87.

18. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، أسيوط: مكتبة الآلات الحديثة، 1996م، ص 92.

ثانيا / المراجع الأجنبية:

1-Alan, Howell: preserving Digital information: challenges and solution, November 2004, P. 4. Available at: www.nla.gov.au/nla.cat-vn3510708

2-Dickman J, Josph C., Charles, EARP, Information Preservation: Changing Roles. Information Management Journal. Lemexa– Nov/ Dec 2002, Vol. 36.Iss. 6Pg. Available At: http://proquest.umi.com

3-David T. Shaw . Electronic Records Management Criteria and Information Security , Australian Information Warfare and Security Conference , 2006.

4-Farmer, Jackie. Information Security: The Nature and Structure of Intrusion Detection Systems, Management Dissertation, Walden University.2006.

5- International Records Council on Archives, Guide of Managing Electronic Records,Canada,2002.

6- Public records office, Management, appraisal and preservation Electronic records, 1999.at: www.nationalarchives.gov.uk

7-Robinson, Stephen and Linda Volonino. Principles and Practices of Information Security. Upper Saddle River, N.J.: Pearson Prentice Hall, 2004.