# أمن المعلومات وإدارة الوثائق: كيف تجمعهما إدارة المخاطر؟

إليسا غارثيا موراليس



**الملخص:**

يناقش المقال التقارب بين إدارة مخاطر المعلومات وأمنها وإدارة الوثائق، والحاجة إلى تعاون مهني لتوجيه قرارات التحول الرقمي. ويعرض توترًا بين الأنظمة المركزية المغلقة وتوسع الأجهزة والخدمات وقنوات التفاعل ومتطلبات الإتاحة، موضحًا أن موقع المؤسسة يختلف بحسب أهدافها ومخاطرها. ثم يربط تقدير المخاطر بأنواع المعلومات وقيمتها ودورات حياتها، ويبرز إسهام تصنيف الوثائق والبيانات الوصفية في تحديد الحماية المناسبة. ويعرض تجربة مصرفية انتقلت من تصور تقني مقيد إلى نموذج مرن لحوكمة المعلومات بمشاركة وحدات متعددة. ويؤكد أن التغيير يحتاج سياسة مشتركة وتدرجًا وتوازنًا بين سرعة حاجات الأعمال وبطء تعديل الأنظمة القائمة، مع بقاء المثال والتوقعات في إطار المصدر التاريخي، وليس وصفًا عامًا لجميع المؤسسات.

**الكلمات المفتاحية:** مخاطر المعلومات، أمن المعلومات، إدارة الوثائق، حوكمة المعلومات، التحول الرقمي

## 1. مقدمة:

نشهد تقاربًا مثيرًا للاهتمام بين مجالات مهنية كان الترابط بينها ضعيفًا تقليديًا. ففي أحدث ملتقى لإدارة المعلومات نظمته (Sedic) عام 2015، شاركت في تبادل ثري لوجهات النظر بين خبراء الأمن وخبراء إدارة المعلومات والوثائق.

وفي الاتجاه نفسه، أعرب (Roger Poole) (2015) في المنتدى المهني لـ (AIIM) عن ثقته بتقارب مهنيي المعلومات والوثائق مع قضايا الأمن وحماية البيانات، وخاصة مع قرب تنفيذ إصلاح خصوصية البيانات في الاتحاد الأوروبي (European Commission, 2015). وقد لمست هذا الاهتمام المتبادل أيضًا في مشروعاتي الاستشارية الأخيرة، أثناء العمل مع فرق متعددة التخصصات لتحديد سياسات حوكمة المعلومات.

## 2. التوترات وتحديات المستقبل:

يشبّه تقرير مهم لشركة (Gartner) الاستشارية (Perkins; Byrnes, 2015) المشهد المستقبلي حتى 2020 بانفجار نجم من نواته نحو أطراف تتمدد باستمرار. ويطرح التشبيه محورين رئيسين للتوتر: الأول بين نواة تسودها نماذج تقنية ومعلوماتية مركزية، وأطراف تتكاثر فيها الأجهزة والتطبيقات ووسائط التخزين والتفاعلات والاتصالات؛ والثاني بين نواة ذات وصول وأمن مغلقين ومنضبطين، وأطراف تتزايد فيها متطلبات الإتاحة والشفافية والانفتاح.

يضع التحول الرقمي المؤسسات أمام قرارات بالغة الأهمية بشأن موقعها على محوري التوتر بين النواة والأطراف. وتتباين النماذج تبعًا لخصائص المؤسسة وحجمها وقطاعها واستراتيجيتها التجارية. وتتعقد القرارات باستمرار، مما يجعل مواءمة الرؤى والتوجهات بين جميع المجالات المهنية المتصلة بإدارة المعلومات ضرورة.

## 3. إدارة المخاطر في صميم القرارات:

كما يوضح (CESG) (2015)، يمثل نظام إدارة مخاطر المعلومات عامل نجاح حاسمًا وعنصرًا محوريًا في أي استراتيجية للأمن السيبراني. لكن لا يبدو ممكنًا تطبيق تدابير أمن بالمستوى نفسه على جميع معلومات المؤسسة إلى ما لا نهاية؛ بل يلزم التمييز بحسب أنواع المعلومات ودورات حياتها. والموازنة بين المخاطر المقبولة وقيمة المعلومات ملازمة لكل قرار في إدارتها وحوكمتها. وهنا تفيد منهجيات إدارة الوثائق والسجلات في تقدير مخاطر الأصول المعلوماتية المختلفة وتقييمها. وتعمل إدارة مخاطر المعلومات بوصفها نقطة التقاء بين التخصصات التي تحمي الشركة من الضرر الأمني المحتمل وتلك التي تتيح تصنيف المعلومات وتحسين تنظيمها واستخراج قيمتها طوال دورة حياتها. ويقدم التقرير الفني (ISO 18128) (Aenor, 2014) ، الذي لا يعرفه مسؤولو الأمن وإدارة المخاطر، إرشادًا لتقدير المخاطر التشغيلية في إدارة المعلومات والوثائق. ومن خبرتي العملية، ينبغي أن تشارك جميع التخصصات المتصلة بالمعلومات في تقييم المخاطر المرتبطة بالسياق.

## 4. التقارب في الممارسة:

للتوضيح، أشير إلى حالة عملية حديثة في القطاع المصرفي. بدأ المشروع بمعالجة إدارة الوثائق بمتطلبات تقوم على استخدام برمجية مركزية لإدارة محتوى المؤسسة (ECM) في بيئة داخلية مقيدة. وبتشبيه التوترات السابق، كان هذا نهج النواة التقليدي. لكن إنشاء فريق استراتيجي يضم مسؤولي المخاطر وأمن المعلومات والامتثال والمسؤولية الاجتماعية والبحث والتطوير وإدارة البيانات والتنظيم والعمليات أظهر سريعًا الحاجة إلى نموذج أشد تحولًا؛ فالواقع يدفع المصارف إلى التوسع نحو الأطراف. ويخضع القطاع المالي لضغط تنظيمي شديد ولديناميات قوية تغير نموذج الخدمة والعلاقة بالعملاء. وقد ظهرت التوترات المذكورة في معظم القرارات المتعلقة بالسياسات والتقنية والتشغيل: ما المعلومات التي ستُخزَّن في حلول التخزين السحابي المختلفة، وكيف تُدار؟

وما المحتويات التي ينبغي أن تبقى في الأنظمة الداخلية بحسب مستويات المخاطر ومتطلبات الأمن؟ وكيف تُسجل أدلة التفاعلات مع الأطراف الأخرى عبر قنوات أو أجهزة متعددة؟ وكيف يُطبق تصنيف موحد للمعلومات وتحديد موحد لمستويات أمنها؟ وكيف تُقدم البيانات الوصفية خدمةً لتطبيقات متعددة؟ وغير ذلك.

كانت النتيجة تحديد نموذج مرن وتكاملي لحوكمة المعلومات يجمع مبادئ الإدارة المشتركة بين إدارة المخاطر وإدارة أمن المعلومات وإدارة السجلات، بمعناها الشامل للبيانات والوثائق. وتُبنى استراتيجية المعلومات على سياسة تحدد معايير أساسية تساعد المصرف على اتخاذ الموقع المناسب بين المركزية واللامركزية والإغلاق

والانفتاح لكل مجموعة أو مجموعة فرعية من المحتويات المعلوماتية. وخُطط للتبني والتحول على خمس سنوات؛ وقد تبدو مدة طويلة قياسًا بسرعة البيئة. لكن تجربتنا العملية تبين أن الإجراءات التي تغير النواة القائمة بطيئة عمومًا، وتأتي استجابةً للتغيرات. ويتمثل التحدي في موازنة هذه التحولات مع الإيقاع الذي تدفع إليه حاجات التوسع نحو الأطراف؛ وهذا يستلزم تعاونًا أوثق باستمرار بين جميع الأطراف المعنية.

## المراجع:


- CESG (2015). 10 Steps to cyber security. The UK National Technical Authority for Information Assurance (formerly Communications-Electronics Security Group). https://www.gov.uk/government/publications/cyberrisk-management-a-board-level-responsibility/10steps-summary
- European Commission (2015). Agreement on Commission's EU data protection reform will boost digital single market. Press release, Brussels, 15 December. http://europa.eu/rapid/press-release_IP-15-6321_ en.htm
- Perkins, Earl; Byrnes, Christian (2015). Cybersecurity scenario 2020 phase 2: Guardians for big change. Gartner. https://www.gartner.com/doc/3097027/cybersecurityscenario--phase-
- Poole, Roger (2015). "The basics and (hopefully) some useful information!". Foro AIIM, December.
- Aenor (2014). UNE-ISO/TR 18128:2014 IN. Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. http://www.aenor.es/aenor/normas/normas/fichanorma.asp? tipo=N&codigo=N0053363


إليسا غارثيا موراليس – http://www.inforarea.es