Politécnico costa atlántica
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

REVISTA GESTIÓN, COMPETITIVIDAD E INNOVACIÓN

Gestión de la seguridad de los activos de la información para la administración pública

Management of the security of the assets of the information for the public administration

Dougglas Hurtado Carmona*

* Doctor en Ciencias, Magister en Ingeniería de Sistemas y Computación, Ingeniero de Sistemas, Universidad Metropolitana, Politécnico de la Costa Atlántica, Barranquilla, Colombia, dhurtado@unimetro.edu.co dhurtadoc@pca.edu.co

Fecha de recepción: 28 de febrero de 2016

Fecha de aceptación: 17 de Junio de 2016

Citación:

Hurtado Carmona, D. (2016). Gestión de la seguridad de los activos de la información para la administración pública. Gestión, Competitividad e innovación(Enero-Junio 2016), 70-77.

RESUMEN

En el presente documento se presentan las estrategias que debe adoptar la administración pública en Colombia como fundamento para aplicar una política de gestión que le permita proteger los activos de la información.

***Palabras Claves**: Gestión, seguridad, activos de la información, administración pública.*

ABSTRACT

This paper presents the strategies to be adopted by the public administration in Colombia as a basis for implementing a management policy that allows it to protect the information assets.

***Keywords**: Management, security, information assets, public administration.*

1. Introducción

En un primer lugar, la Ley 594 DE 2000 fue legislada con el fin de establecer las pautas y preceptos generales que regulan la función archivística del estado colombiano, aplicable a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por dicha ley. Esta misma ley, le delega la salvaguarda del patrimonio documental colombiano, así como a la modernización de los archivos públicos, al Archivo General de la Nación (AGN). Este a su vez, para cumplir con el ordenamiento se orienta a fortalecer y actualizar los lineamientos relativos al patrimonio documental.

De manera transversal, la gestión documental, en Colombia, se encuentra inmersa en las iniciativas de gobierno electrónico y en la apropiación de tecnologías de la información y la comunicación (TIC) en la administración pública, como parte de la estrategia estatal de ofrecer servicios de calidad con una marcada transparencia. Con esto, el estado colombiano pretende brindar acceso a los ciudadanos del patrimonio documental en forma expedita y transparente.

En esta misma línea y desde el punto de vista de la Unesco, el patrimonio documental de un país lo representan contenido y el soporte en el que se deposita, de allí, la clasificación que hace de ellos: Piezas textuales con un contenido que en su mayoría está constituido por símbolos que representan fonemas; Piezas no textuales identificados como dibujos y similares; Piezas audiovisuales en base al sonido y a los fotogramas; y Documentos virtuales, que se encuentran almacenados en distintos dispositivos electrónicos.

Debido al creciente uso de los documentos virtuales por medio de internet, nacen nuevas conductas que atentan contra la integridad, disponibilidad, confidencialidad, autenticidad y derechos de autoría de la información contenida en dichos documentos. Ante esto, el estado Colombiano implementó medidas coercitivas, con la que se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", y tipificando como delitos una serie de conductas que atentan la seguridad de la información. Esta medida se conoce como la Ley 1273 de 2009.

2. Problemática

En Colombia se tiene una legislación que regula el cómo deben ser archivados el patrimonio documental en la administración pública, y también se tiene una legislación que permite castigar a los que comentan delitos en contra de los contenidos del patrimonio documental. Esto se puede traducir en que existe una política de estado que permite a las entidades públicas administrar el patrimonio documental y a su vez castigar a los que atenten contra este patrimonio.

Pero si observamos el hecho, dado que la Ley 1273 trata sobre "protección de la información y de los datos", y proteger es procurar, mediante cualquier medio, que algo se conserve en buenas condiciones, se nota que la información y los datos no está siendo protegida. Porque cuando se aplica esta Ley (o el código penal más específicamente), ya la información (contenido del patrimonio documental) ha sido quebrantada en su integridad, disponibilidad, autenticidad, confidencialidad o en todas ellas. Es decir, que esta ley no protege a la información ni a los datos, porque es un post-control. Ahora bien, con esto queda claro que se hace necesaria una política de estado que resguarde la seguridad de la información y de los datos en la administración pública, para así poder contribuir a la concientización de la existencia de un activo intangible denominado activos de la información, que debido a su valor estratégico y de ventaja competitiva, el estado debe proteger.

3. Estrategias

La administración pública en Colombia debe tener un conocimiento exacto sobre los activos de información que posee, como parte importante de la gestión de riesgos. Además, los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen. También deben ser rotulados para estipular cómo se deben tratar y proteger.

Habitualmente, la información deja de ser crítica o confidencial después de cierto período de tiempo o cuando ya se ha hecho pública. Estas particularidades deben tenerse en cuenta para evitar el exceso de clasificación y gastos innecesarios. Asimismo, la información adopta muchas formas, medios de almacenamiento y de trasmisión, y en cada una, se deben contemplar los mecanismos de protección asegurar se confidencialidad, integridad y disponibilidad. Finalmente, la información puede convertirse en obsoleta y se hace necesario eliminarla, en un proceso que debe asegurar la confidencialidad de la misma.

De lo anterior se estima que se hace necesario que la administración pública en Colombia tenga una gestión de los activos de información como estrategia metodológica, que permita gestionar los activos de información, en la cual se deben tener en cuenta los siguientes objetivos a cumplir:

Responsabilidad por los Activos. Este objetivo se encuentra centrado en lograr mantener la protección adecuada de los activos de la administración pública. Para esto, es necesario que cada uno de los activos de información se involucre y se le asigne un dueño. Cada dueño de cada activo tiene la responsabilidad de la gestión de los controles apropiados.

Clasificación de la Información. Con este objetivo se busca que la información reciba el nivel de protección adecuado. Este objetivo se orienta a descubrir las necesidades, las prioridades y el nivel necesario de protección.

Para poder lograr estos objetivos se puede realizar un procedimiento dividido en las siguientes etapas:

1. Identificación de activos. Se identifican los activos de información, en base a la definición de qué es y qué no es. Se unifican a todos aquellos que tengan características comunes y que posean el mismo nivel de seguridad. El producto de esta etapa es un inventario estructurado de activos de información.
2. Análisis de riesgo de los activos de información. A cada activo de información se realiza la evaluación en donde se identificación de los riesgos tecnológicos a los que está expuesto y la medición de riesgos identificados.
3. Gestión de activos. En esta etapa se categorizan los activos en cuento a su grado de sensibilidad frente a sus riegos.
4. Control y seguimiento. En esta etapa se busca detectar desviaciones o ajustes necesarios a los planes de mitigación de riesgos.

4. Política para la gestión de activos de la información

Una política para la gestión de activos de información que preserve el patrimonio documental de nación en la administración pública, debe estar en sinergia con las leyes 594 DE 2000 y 1273 de 2009, pero, a su vez, complementar el control y la protección definiendo las responsabilidades y procedimientos para el manejo de la información según su sensibilidad e impacto ante un incidente de seguridad. Esta política debe estar enmarcada en los aspectos numerados y descritos a continuación:

4.1 Objetivo, alcance y usuarios

Los objetivos centrales que se buscan por intermedio de la gestión de activos de la información se enfocan primero en garantizar que los activos de información reciban un nivel de protección apropiado y segundo en clasificar la información de manera que permita determinar su grado de sensibilidad y de criticidad. También es importante señalar que, dependiendo de esta clasificación, se definen los mecanismos de protección a cada activo.

Una Política de este tipo se aplica a toda la información administrada por las instituciones públicas y privadas que tienen funciones públicas en Colombia, cualquiera sea el soporte en que se encuentre. Los usuarios a los cuales atañe son todos los empleados de las instituciones que manejen el patrimonio documental de la nación.

4.2 Documentos de referencia

Los documentos de referencia que serán tenidos en cuenta son: Norma ISO/IEC 27001, puntos A.7.2.1, A.7.2.2, A.10.7.1, A.10.7.3, A.10.7.4, A.10.8.4 y A.11.6.1; Política del sistema de gestión de seguridad de la información; Informe sobre la evaluación de riesgos; Declaración de aplicabilidad; Inventario de activos; Lista de obligaciones estatutarias, legales y contractuales; Procedimiento para gestión de incidentes; toda legislación que regula la clasificación de información. Algunos documentos opcionales serían: Procedimientos operativos para tecnología de la información y de la comunicación; Política de eliminación y destrucción; obligaciones contractuales que regulan la clasificación de información.

4.3 Información clasificada

Pasos y responsabilidades

Los Propietarios de los Activos de la información son los autorizados de clasificar, documentar y mantener actualizada la clasificación realizada, asimismo, definir las autorizaciones de acceso a los activos y mantener los mecanismos de control. El Responsable de la Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan. Los pasos y responsabilidades para la gestión de la información son los siguientes:

Tabla 1. Pasos y responsabilidades. FuenteElaboración Propia (2016)

Nombre del paso	*Responsabilidad*
Ingreso del activo de información en el Inventario	Director de Seguridad de la información o similar
Clasificación de la información	Propietario del activo
Etiquetado de la información	Propietario del activo
Manejo de la información	Personas que poseen derechos de acceso sobre el activo

Si la información clasificada proviene de afuera de la institución, el director de seguridad de la información es el responsable de su clasificación, y se convierte en el propietario de ese activo de información.

Clasificación de la información

Los criterios de clasificación son los siguientes:

Confidencial: Constituye una información de un nivel de sensibilidad alto, con un alto impacto ante un incidente de seguridad, la cual solo debe ser accesada en la forma adecuada, por usuarios autorizados por el propietario del activo de información. Una información confidencial debe ser protegida en su almacenamiento y transmisión, y requiere el consentimiento formal del Propietario para su divulgación.

Uso interno: Es la información dispuesta de ser comunicada internamente sin restricciones, y sólo podrá ser difundida a un tercero cuando preliminarmente exista autorización del Propietario para su entrega, que en todo caso deberá acreditarse.

Pública: Es aquella información cuya difusión pública ha sido aprobada. por el Propietario de la información.

Etiquetado de la información

Toda información, ya sea confidencial, uso interno o pública, debe ser rotulada de acuerdo al estándar definido, independientemente de estar almacenada en distintos medios. Además, se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido.

Manejo de información clasificada

Se deben estipular procedimientos y mecanismos de control en el manejo de la información, según su clasificación, en especial en los siguientes procedimientos:

1. Copiado e Impresión de Información confidencial
2. Almacenamiento de Información
3. Autorización de Acceso a Información sensible.
4. Manejo de Información Confidencia en Reuniones
5. Derecho a Saber
6. Consideraciones de acceso a computadores y de red.

4.4. Cumplimiento

Si algún miembro del personal de administración o de función pública se encuentra que ha violado esta política, puede ser sujeto a una acción disciplinaria y las demás acciones que dictamine la ley.

4.5 Validez y gestión de documentos

La política es aplicable a partir de su aprobación y publicación, la cual se realizará por los medios destinados para tal fin por el gobierno nacional. Esta política será revisada cuando se considere apropiado, pero el periodo no puede exceder los 12 meses. La revisión de la política estará a cargo del Ministerio de Tecnologías de la Información y Comunicaciones.

Referencias

Ley 594. (2000). Diario oficial Congreso de la República de Colombia.

Norma ISO/IEC 27001. (2005). International Organization for Standardization.

Ley 1273. (2009). Diario oficial Congreso de la República de Colombia.

American National Standards Institute. (2004). American National Standard for Information Technology –. Role Based Access Control. ANSI INCITS 359-2004. New York: American National Standards Institute, Inc.

Archivo General de la Nación - Colombia. (2014). Politicas de Archivo. Recuperado el 24 de junio de 2014, de Politicas - Archivo General de la Nación: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/GestionDocumental/05_politica_archivos.pdf

Brose, G. (2001). Access Control Management in Distributed Object Systems (Doctoral Dissertation) . Berlin: Freie Universität Berlin.

Calder, A., & Watkins, S. (2010). Information Security Risk Management for ISO27001 / ISO27002. IT Governance Ltd.

Chen, L. (2011). Analyzing and Developing Role-Based Access Control Models (Doctoral Thesis). London: University of London.

Ferreiolo, D. F., & Kuhn, D. R. (1992). Role-Based Access Controls. Proceedings National Computer Security Conference, (págs. 554-563).

Forrester, J. W. (1961). Industrial Dynamics. Massachuset: MIT Press.

Gibson, D. (2012). Access Control. En D. Gibson, CISSP Rapid Review (págs. 1-24). Microsoft Press.

Hurtado Carmona, D. (2011). General Systems Theory A focus on computer science engineering. Raleigh: Lulu Publishers.

Instituto Colombiano de Normas Técnicas - Icontec. (2011). Sistema de Gestión de la Seguridad de la Información (SGSI). Bogotá: Icontec.

Instituto Colombiano de Normas Técnicas Icontec. (2005). Norma Técnica Colombiana NTC-ISO 9000. Bogotá: Icontec.

International Organization for Standardization ISO. (1998). ISO/IEC 2382-8:1998. Information technology -- Vocabulary. Ginebra: ISO/IEC.

International Organization for Standardization ISO. (2005). ISO 9001 Quality Management System. Fundamentals and vocabulary. ISO/IEC.

International Organization for Standardization ISO. (2008). ISO/IEC 27005:2008. Risk management in information security. Ginebra: ISO/IEC.

Lobel, J. (1986). Foiling the System Breakers: Computer Security and Access Control . New York: McGrawHill Book Company.

Ministerio de Hacienda y Administraciones Públicas. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT – Versión 3.0. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. Gobierno Espñol.

Ministerio de Salud. Gobierno de Chile. (2011). Política de seguridad en la clasificación y manejo de la información. Santiago de Chile: Gobierno de Chile.

Mitnick, K., & Simon, W. (2003). The art of deception. Controlling the Human Element of Security. Wiley.

Morin, E. (2009). Introducción al pensamiento complejo. Barcelona: Gedisa.

Munawer, Q. (2000). Administrative Models for Role-Based Access Control (Doctoral Thesis). Fairfax, Virginia: George Mason University .

Oficina Nacional de Tecnología de Información ONTI. (2012). Politica de seguridad de la información para organismos de la administración pública nacional. Versión 3.2. Buenos Aires: República de la Argentina.

Ruskwig. (2011). Choosing A Secure Password, User Responsibilities. Recuperado el 25 de mayo de 2014, de http://www.ruskwig.com/docs/passwords_policy.pdf

Ruiz López, D., & Cardénas Ayala, C. (2005). ¿Qué es una política pública? UIS Revista Juridica, V.

Ruskwig. (2011). I.T. SECURITY POLICY. Recuperado el 26 de mayo de 2014, de http://www.ruskwig.com/docs/security_policy.pdf

Ruskwig. (2011). IT Security policy. Recuperado el 26 de mayo de 2014, de http://www.ruskwig.com/docs/security_policy.pdf

Ruskwing. (2011). Remote Access Security Policy. Recuperado el 26 de mayo de 2014, de http://www.ruskwig.com/docs/remote_policy.pdf

Schneider, F. B. (2012). Chapter 7. Discretionary Access Control. Obtenido de Cornell University: https://www.cs.cornell.edu/fbs/publications/chptr.DAC.pdf

Shannon, C. (1948). A Mathematical Theory of Communication. The Bell System Technical Journal, 27 , 379–423, 623–656.

Stone, C. (2010). Information Security Policy. Security Policy Template. Recuperado el 27 de mayo de 2014, de ruskwig.com: http://www.ruskwig.com/docs/iso-27002/Information%20Security%20Policy.pdf

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. Gaithersburg: National Institute of Standards and Technology.

Toahchoodee, M. (2010). Access control models for pervasive computing environments . Fort Collins: Colorado State University.

U.S. Department of Commerce. NIST. (2011). Managing Information Security Risk. Organization, Mission, and Information System View. NIST Special Publication 800-39. Gaithersburg: National Institute of Standards and Technology.

U.S. Department of Commerce. NIST. (2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. Gaithersburg: National Institute of Standards and Technology.

Vanderbosch, C. (2002). Manual avanzado de investigacion policiaca/ Advanced Manual of Police Investigation. Editorial Limusa S.A. De C.V.

Zhou, W. (2008). Access Control Model and Policies for Collaborative Environments (Doctoral Dissertation). Potsdam : Universitaet Potsdam.