DIRECCIÓN DE INFORMÁTICA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Secretaría de Gestión Humana y Desarrollo Organizacional

Gobernación de Antioquia

2018

Luis Eduardo Corredor Bello

Director Técnico de Informática

Equipo de profesionales
especializados y universitarios

Dirección de Informática
Calle 42 B 52 - 106 Piso 2, costado occidental Tel:
(4) 3838910 - Fax 3811253 Centro Administrativo
Departamental José María Córdova (La Alpujarra)
Medellín - Colombia – Suramérica

CONTENIDO

CONTROL DE CAMBIOS

Fecha	Versión	Estado	Descripción del cambio
Febrero de 2018	1	Publicada	Generación de un nuevo documento "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información"

INTRODUCCIÓN

La información es un activo de alto valor para la Gobernación de Antioquia. A medida que los procesos de la entidad se hacen más dependientes de la información y de las tecnologías que la soportan, se hace necesario contar con actividades de planeación estratégica que, en concordancia con la política de seguridad de la información institucional, permitan el tratamiento (principalmente la mitigación) riesgos y la atención a las necesidades de seguridad de la información de la entidad.

El presente documento indica de forma general el tratamiento, es decir, las actividades para mitigar los riesgos identificados de seguridad de la información, así como también, las actividades para atender los requerimientos institucionales de seguridad de la información. Entendiendo que el presente documento es de naturaleza pública, se evitará la descripción detallada de las actividades y controles de seguridad empleados ya que a partir de ellas se podrá inferir la existencia de condiciones de seguridad que pueden ser aprovechadas por amenazas externas.

1. OBJETIVO

Establecer y formalizar de forma general el tratamiento de riesgos de seguridad de la información, Gobernación de Antioquia.

2. ALCANCE

El documento abarca procedimiento para el tratamiento de los riesgos y necesidades de la seguridad de la información con su respectivo plan de acción, responsable, duración estimada e importancia (prioridad)

3. MARCO NORMATIVO

3.1 Decretos y leyes que aplican

- La Ley 1712 de 2014. “Ley de transparencia y del derecho de acceso a la información pública nacional”.
- La Ley 1581 de 2012 y decreto 1377 de 2013. “Ley de protección de datos personales”.
- La Ley 1273 de 2009. “Ley de delitos informáticos y la protección de la información y de los datos”.
- Decreto 1078 del 26 de mayo de 2015. Por medio del cual se expide el “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- La Ley 527/1999. “Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- Decreto 612 del 4 de abril de 2018, "por el cual se fijan directrices para la integración de planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado".
- Decreto 1008 del 14 de junio de 2018, "Por el cual se establecen los lineamientos generales de la política Gobierno Digital”.

3.2 Bases metodológicas.

- ✓ Norma ISO/IEC 27001:2013.
- ✓ Modelo de Seguridad y Privacidad de la Información de Gobierno Digital –MSPI.

4. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Gobernación de Antioquia

Por motivos de confidencialidad de los controles y las medidas específicas para tratar los riesgos de seguridad de la información, el plan de tratamiento de riesgos se describirá de forma general, indicando las macro-actividades encaminadas a mitigar cada riesgo, así como a dar cumplimiento a los requisitos de seguridad de la información.

#	Actividad	Descripción	Impor-tancia	Resp. Principal	Riesgo o requerimiento asociado	Duración en días
1.	Gestión de la seguridad de la información	Mejora del esquema de gestión de seguridad de la información institucional, buscando el cumplimiento del MSPI y la norma internacional de gestión ISO/IEC 27001	1	Equipo de seguridad	REQ1. Norma ISO/IEC 27001:2013 y MSPI	43
2.	Implementaciones técnicas	Implementación y mejora de herramientas tecnológicas para la mitigación de riesgos de ciberseguridad	1	Profesional Universitario	Riesgo #1152 Acceso Ilegal	81
3.	Construcción de la arquitectura de seguridad	Construcción de un esquema que permita el entendimiento y la mejora de la postura de seguridad institucional	2	CISO	REQ3. Arquitectura de seg. de la información	17
4.	Gestión de vulnerabilidades	Identificación y seguimiento a la solución de vulnerabilidades	2	Profesional Universitario	Riesgo #1152 Acceso Ilegal	45
5.	Mejora de la gestión del acceso	Identificación de brechas y posterior mejora de la gestión de acceso e identidades	3	CISO	Riesgo #1152 Acceso Ilegal	25

#	Actividad	Descripción	Impor-tancia	Resp. Principal	Riesgo o requerimiento asociado	Duración en días
6.	Continuidad de los servicios de seguridad de la información	Definición de planes de actuación ante la interrupción de los servicios tecnológicos de seguridad de la información.	2	CISO	Riesgo #1178 No operación parcial o total de la infraestructura de TIC	25
7.	Toma de conciencia	Transmisión de mensajes enfocados en actuaciones correctas y responsables frente a la seguridad de la información por parte de los servidores públicos y usuarios de la información institucional.	3	Profesional Universitario	Riesgo #1152 Acceso Ilegal	31
8.	Diagnósticos externos y pruebas de concepto	Identificación y evaluación de tecnologías de seguridad de la información que podrían ser usadas para el tratamiento de riesgos de ciberseguridad	3	CISO	REQ4. Mejorar la seguridad tecnológica	15
	TOTAL					282,00