DIRECCIÓN DE INFORMÁTICA

PLAN DE LA 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 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 control y administración efectiva de los riesgos y de las necesidades de seguridad de la información de la entidad.

El presente documento detalla la planeación de la gestión de la seguridad y privacidad de la información, ejercicio que es coordinado y aprobado por el Comité de Dirección de Seguridad de la Información -CDSI.

1. OBJETIVO

Establecer y formalizar la planeación y ejecución de la gestión de la seguridad de la información en concordancia con los riesgos y necesidades asociadas, en la Gobernación de Antioquia.

2. ALCANCE

El documento abarca la planificación de la seguridad de la información desde la identificación de factores internos y externos (amenazas y vulnerabilidades) hasta la definición de objetivos y macro actividades relacionadas a ser ejecutadas.

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 Seguridad y Privacidad de la Información – Gobernación de Antioquia

El plan establece la ruta a seguir en cuanto a la gestión de seguridad de la información con base en la definición de prioridades. El punto de partida de la estrategia es la identificación de problemas internos (vulnerabilidades) y externos (amenazas) a partir de los que se podrán definir los riesgos de seguridad de la información.

4.1 Problemas de seguridad y privacidad de la información

A continuación, se relacionan las amenazas y vulnerabilidades identificadas en la administración departamental, con los cuales de concretan 2 potenciales riesgos: “Acceso Ilegal” y “No operación parcial o total de la infraestructura de TIC”:

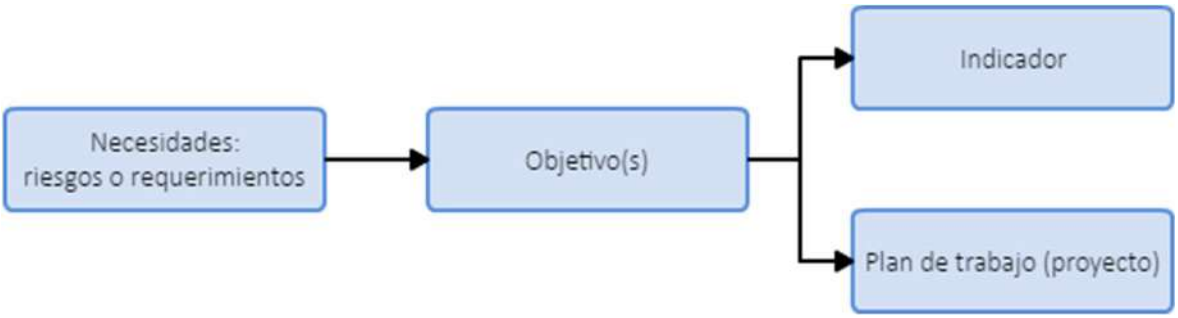
Problemas		
Vulnerabilidades	Amenazas	Riesgos
1. Demora en el cierre de vulnerabilidades identificadas. 2. Dificultades para detección de ataques. 3. Ausencia de requisitos y estándares de configuración segura. 4. Dificultades para el control de acceso a la red interna. 5. Dificultades para detectar y priorizar las vulnerabilidades de la infraestructura de TIC. 6. No se gestionan de manera consistente los incidentes de seguridad de la información 7. Vulnerabilidades de la aplicación web (como inyección de código, cross site scripting y acceso ilegal a recursos). 8. El tráfico de la mayoría de sitios web no viaja cifrado entre el servidor y el usuario del sitio. 9. Configuración o instalación insegura del servidor web (apache, tomcat, IIS, glassfish, entre otros) o del gestor de contenido (joomla, wordpress, drupal, entre otros). 10. Las diferentes áreas de la entidad contratan la adquisición (o desarrollo) de aplicaciones sin exigir el cumplimiento de	1. Delincuentes informáticos. 2. Software Malicioso. 3. Áreas de la entidad que requieren la aprobación o aceptación de sistemas que no cuentan con seguridad mínima necesaria. 4. Delincuentes informáticos que planean ataques de seguridad aprovechando las debilidades en la cultura de seguridad de las personas. 5. La posible existencia de administradores de TIC que realicen actividades irresponsables o indebidas, o de personas no autorizadas que conocen sus credenciales. 6. Personas no autorizadas (como delincuentes informáticos) que buscan robar las credenciales de los administradores de las TIC. 7. Usuarios internos de la entidad que pueden de manera intencionada o no intencionada, borrar, acceder o eliminar un archivo.	Riesgo #1152 Acceso Ilegal

Problemas		
Vulnerabilidades	Amenazas	Riesgos
requisitos de seguridad ni la realización de pruebas. 11. No es posible registrar (grabar) los accesos de los usuarios administradores. 12. Los cambios en el Directorio Activo no quedan registrados y no son auditados. 13. Los cambios en el Firewall no quedan registrados y no son auditados. 14. Los administradores debe utilizar múltiples credenciales para los sistemas que administran, situación que facilita que compartan credenciales, que las escriban, o que utilicen la misma para múltiples sistemas. 15. No es posible determinar la identidad de un usuario previamente autorizado que accede, modifica o borra un archivo en las carpetas red. 16. Personas no autorizadas acceden a los archivos del servidor de carpetas red. 17. Los usuarios de Office 365 no aplican consistentemente los controles de acceso a archivos. 18. El procedimiento de gestión de acceso no contempla las actividades de retiro de derechos de acceso de personas que se retiran de la organización. 19. No hay una fuente de información centralizada que permita identificar de forma confiable que un contratista se retiró de la entidad. 20. Cultura débil en seguridad de la información: desconocimiento o desestimación de las buenas prácticas de seguridad de la información durante las actividades laborales por parte de los usuarios de la información (servidores públicos, contratistas, practicantes). 21. Cultura débil de seguridad por parte de los directivos de la organización, lo	8. Exempleados o ex contratistas que intentan acceder a las tecnologías de la información y la comunicación de la entidad.	

Problemas		
Vulnerabilidades	Amenazas	Riesgos
que impide aplicar de manera eficaz las iniciativas de cultura en seguridad de la información.		
1. Ausencia de lineamientos o instrucciones formales para atender una situación de falla o interrupción en la operación de las tecnologías de seguridad de la información. 2. Las implementaciones sencillas (con un único punto de falla) no entregan el nivel de disponibilidad requerido por la entidad.	1. Errores Humanos (por ejemplo: en la administración de los sistemas). Fallas en las tecnologías de seguridad de la información. 2. Fallas en las tecnologías de seguridad de la información.	Riesgo #1178 No operación parcial o total de la infraestructura de TIC *(riesgo identificado para todo el proceso PATIC)*

4.2 Estrategia para mitigar los riesgos encontrados.

La estrategia presenta el estado actual en lo relacionado a riesgos dentro del alcance del SGSI y el estado planeado al final de su ejecución, está definida con base dos tipos de necesidades de seguridad de la información de la entidad: riesgos y requerimientos (de las partes interesadas). El plan de seguridad y privacidad de la información se construyó a través de un despliegue estratégico esquematizado a continuación:



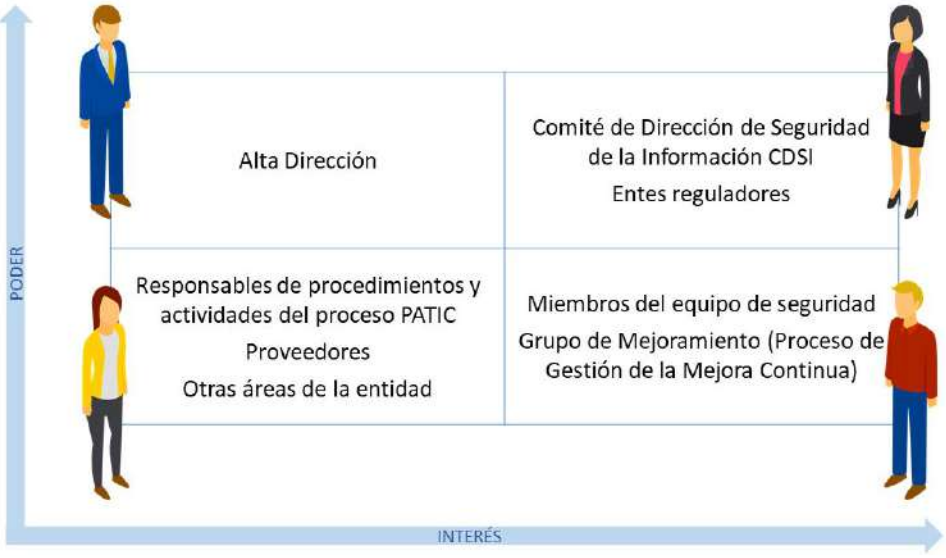
4.3 Mapa de riesgos

Se analizan los dos riesgos potenciales: “Acceso Ilegal” y “No operación parcial o total de la infraestructura de TIC” en el mapa de calor establecido por la entidad como se presenta en la siguiente gráfica:

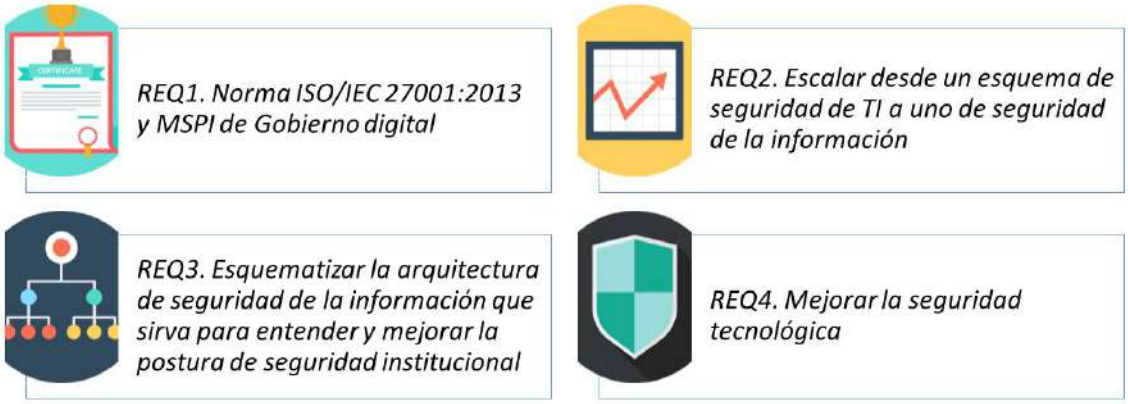
		Impacto				
		1 Mínimo	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
Probabilidad	5 Altamente probable	5 Alto	10 Alto	15 Extremo	20 Extremo *Acceso Ilegal* Mitigar	25Extremo
	4 Probable	4 Moderado	8 Alto	12 Alto	16 Extremo	20 Extremo
	3 Ocasional	3 Bajo	6 Moderado	9 Alto	12 Extremo	15 Extremo
	2 Remota	2 Bajo	4 Bajo	6 Moderado	8 Alto	10 Extremo Mitigar
	1 Improbable	1 Bajo	2 Bajo	3 Moderado	4 Alto	5 Alto *No operación de infrae. TIC*

4.4. Partes Interesadas

Se relacionan en el siguiente mapa, los interesados en cuanto al nivel de poder e interés en la seguridad y privacidad de la información:



4.5 Requerimientos de las partes interesadas



Habiendo definido tanto los riesgos como los requerimientos de las partes interesadas, es posible definir la estrategia (plan) de seguridad y privacidad.

5. ESTRATEGIA DE SEGURIDAD

Necesidad: riesgo o requerimiento	Objetivo(s)	Indicador	Macro-actividad en el programa de estratégico de seguridad (PESI)
Riesgo #1152 Acceso Ilegal	1. Proteger las TIC de la Gobernación de Antioquia de accesos no autorizados. 2. Gestionar de forma eficaz y eficiente las vulnerabilidades técnicas. 3. Mejorar el control de acceso a la plataforma de TIC. 4. Contener la proliferación de software malicioso. 5. Implementar eficazmente una cultura organizacional de	Cobertura de sitios asegurados Gestión de las vulnerabilidades Avance en las actividades de gestión de acceso planeadas Gestión de software malicioso Avance en las iniciativas de toma de conciencia Oportunidad en la gestión de incidentes	Implementaciones técnicas Gestión de vulnerabilidades Mejora de la gestión del acceso

	seguridad de la información. 6. Gestionar adecuadamente los incidentes de seguridad.		
Riesgo #1178 No operación parcial o total de la infraestructura de TIC	7. Definir planes de acción ante interrupciones de tecnologías de seguridad de la información	Avance en la definición de planes	Continuidad de los servicios de seguridad de la información
REQ1. Norma ISO/IEC 27001:2013 y MSPI	8. Cumplir el modelo de seguridad y privacidad de la información	Cumplimiento del ISO 27001	Gestión de la seguridad de la información
REQ2. Escalar desde un esquema de seguridad de TI a uno de seguridad de la información.	9. Definir un mecanismo que permita identificar los riesgos de seguridad de la información en los procesos del SIG.	Inclusión de los riesgos de seguridad de la información en el procedimiento de administración del riesgo	Definición de riesgos de seguridad de la información aplicables a todos los procesos del SIC.
REQ3. Esquematizar la arquitectura de seguridad de la información que sirva para entender y mejorar la postura de seguridad institucional	10. Ilustrar la arquitectura de seguridad de la información.	Arquitectura de seguridad de la información institucional construida y aprobada	Construcción de la arquitectura de seguridad
REQ4. Mejorar la seguridad tecnológica	11. Investigar nuevas herramientas técnicas que incrementen el nivel de seguridad de TIC en la entidad.	Nivel de avance en la realización de pruebas de concepto	Diagnósticos externos y pruebas de concepto