Andrés Orlando López Luján
Secretario de Tecnologías de la información y las Comunicaciones

Patricia Restrepo Vélez
Directora de Tecnología e Información

Gobernación de Antioquia
2021 - 2023

Plan de Identificación y Tratamiento de Riesgos para la 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 inicio de la estrategia es la identificación de problemas internos (vulnerabilidades) y externos (amenazas) a partir de los que se definen los riesgos de seguridad de la información de la Entidad.

Vulnerabilidades	Amenazas	Riesgos
1. Vulnerabilidad de los componentes tecnológicos frente a la dinámica de los atacantes. 2. Ataques informáticos a la infraestructura y sistemas de información de TIC. 3. Abuso y exceso de privilegios. 4. Falta de concientización sobre la seguridad de la información. 5. Obsolescencia tecnológica.	1. Ataques cibernéticos. 2. Ausencia de Segregación de funciones. 3. No actualización de plataforma tecnológica. 4. Software Malicioso. 5. Sistemas que no cuentan con la seguridad mínima necesaria. 6. Debilidades en la cultura de seguridad de la información de los servidores públicos. 7. Préstamo de usuarios entre los servidores públicos. 8. Personas no autorizadas que buscan robar las credenciales de los administradores de las TIC. 9. Usuarios internos de la entidad que pueden de manera intencionada o no intencionada, borrar,	Acceso Ilegal.

Vulnerabilidades	Amenazas	Riesgos
	acceder o eliminar un archivo. 10. Exservidores públicos que intentan acceder a las tecnologías de la información y la comunicación de la entidad. 11. Ausencia contraseñas robustas.	
1. Fallas físicas, lógicas y/o obsolescencia en la infraestructura de TI. 2. Ausencia de BCP/DRP ante un evento catastrófico natural o causado por el hombre (terremoto, incendio, bomba, apagón, etc.) 3. Deficiencia en la documentación del servicio TI y de la planeación para la ejecución de cambios en la plataforma tecnológica. 4. Falla en la prestación de los servicios de terceros (internet, servicios en la nube).	1. Errores Humanos (por ejemplo: en la administración de los sistemas). 2. Fallas tecnológicas por actividades intencionales de servidores públicos o personal externo (Terceros). 3. Fallas tecnológicas por eventos naturales. 4. Ataques cibernéticos que afectan la disponibilidad de la información.	Interrupción de los servicios TIC por problemas asociados a la plataforma tecnológica.
1. Cuentas especiales o genéricas no administradas correctamente. 2. No aplicación rigurosa de la política de seguridad de la información (no compartir contraseñas y revisión periódica y modificación de roles o permisos de acceso).	1. Accesos no autorizados a información sensible de la Entidad. 2. Errores o no actualización de la definición de segregación de funciones. 3. Servidores públicos y/o terceros mal intencionados que alteran información. 4. Ataques de ingeniería social a servidores públicos para acceder a información sensible.	Manipulación indebida de la información para beneficio personal o de terceros.

Vulnerabilidades	Amenazas	Riesgos
	5. Ataque cibernético que afecte directamente la integridad de la información.	

Tabla 1 - Problemas de seguridad (amenazas y vulnerabilidades)

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 identificación y tratamiento de riesgos para la de seguridad y privacidad de la información se construyó a través de un despliegue estratégico esquematizado a continuación:

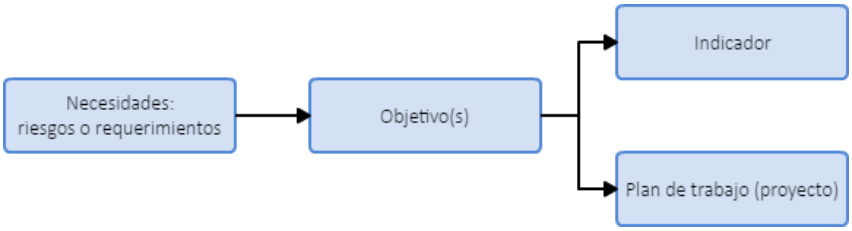

Ilustración 1 - Despliegue esquemático Necesidades de la Entidad

Mapa de riesgos de seguridad de la información para el alcance del SGSI

		Impacto				
		1. Mínimo	2. Menor	3. Moderado	4. Mayor	5. Catastrófico
Probabilidad	5. Altamente probable	5 Alto	10 Alto	15 Extremo	20 Extremo	25 Extremo
	4. Probable	4 Moderado	8 Alto *Acceso Ilegal*	12 Alto	16 Extremo	20 Extremo
	3. Ocasional	3 Bajo	6 Moderado	9 Alto *Manipulación Información*	12 Extremo	15 Extremo
	2. Posible	2 Bajo	4 Bajo	6 Moderado	8 Alto	10 Extremo
	1. Improbable	1 Bajo	2 Bajo	3 Moderado	4 Alto	5 Alto *Interrupción de la Operación*

Ilustración 2 - Mapa de riesgos de seguridad de la información para el alcance del SGSI

Partes interesadas

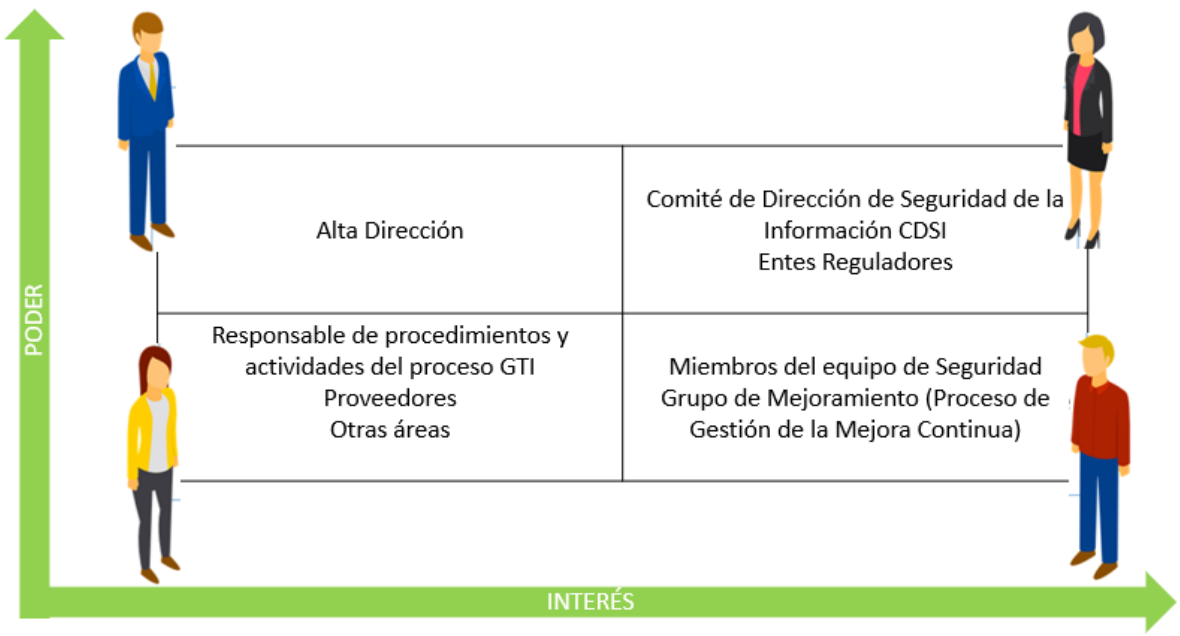

Ilustración 3 - Partes Interesadas

Requerimientos de las partes interesadas

Ilustración 4 -Requerimientos de las partes interesadas

Estrategia de Seguridad

Necesidad: riesgo o requerimiento	Objetivo	Indicador	Macro-Actividad en el Programa de Estratégico de Seguridad (PESI)
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 seguridad de la información. 6. Gestionar adecuadamente los incidentes de seguridad.	1. Tendencias de Eventos de Ambientes Web. 2. Tipo de Ataque vs Mes del Evento identificado. 3. Tipo de Ataque vs Mes del Evento identificado. 4. Eventos de EndPoint. 5. Eventos de Office 365.	Implementaciones técnicas. Gestión de vulnerabilidades. Mejora de la gestión del acceso.
Interrupción de los servicios TIC por problemas asociados a la plataforma tecnológica.	7. Definir planes de acción ante interrupciones de tecnologías de seguridad de la información.	1. Tendencias de Eventos de Ambientes Web. 2. Tipo de Ataque vs Mes del Evento identificado. 3. Tipo de Ataque vs Mes del Evento identificado.	Continuidad de los servicios de seguridad de la información.

Necesidad: riesgo o requerimiento	Objetivo	Indicador	Macro-Actividad en el Programa de Estratégico de Seguridad (PESI)
		4. Eventos de EndPoint. 5. Eventos de Office 365	
Manipulación indebida de la información para beneficio personal o de terceros.	8.1. Definir e implementar controles de acceso eficientes para los sistemas de información. 8.2. Establecer control de usuarios activos. 8.3. Emplear una correcta segregación de funciones para los servidores públicos acorde a su cargo y responsabilidades. 8.4. Definir e implementar logs de auditoría sobre los sistemas de información, bases de datos y sistemas operativos.	1. Tendencias de Eventos de Ambientes Web. 2. Eventos de EndPoint. 3. Eventos de Office 365.	Gestión de vulnerabilidades. Mejora de la gestión del acceso.
REQ1. Norma ISO/IEC 27001:2013 y MSPI de Gobierno Digital.	9. Cumplir el modelo de seguridad y privacidad de la información de Gobierno en Línea.	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.	10. 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.

Necesidad: riesgo o requerimiento	Objetivo	Indicador	Macro-Actividad en el Programa de Estratégico de Seguridad (PESI)
REQ3. Esquematizar la arquitectura de seguridad de la información que sirva para entender y mejorar la postura de seguridad institucional.	11. 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.	12. 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.

Tabla 2- Estrategia de seguridad

Plan de Tratamiento de Riesgos de Seguridad 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 para cada riesgo o requisito de seguridad de la información en la vigencia 2021 a 2023.

#	Actividad	Descripción	Resp. Principal	Riesgo o requerimiento asociado
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.	Equipo de seguridad	REQ1. Norma ISO/IEC 27001:2013 y MSPI
2.	Implementaciones técnicas.	Implementación y mejora de herramientas tecnológicas para la mitigación de riesgos de ciberseguridad.	Equipo de seguridad	- Riesgo Acceso Ilegal - Riesgo Manipulación indebida de la información para beneficio personal o de terceros.
3.	Construcción de la arquitectura de seguridad.	Construcción de un esquema que permita el entendimiento y la mejora de la postura de seguridad institucional.	Equipo de seguridad	REQ3. Arquitectura de seguridad de la información.
4.	Gestión de vulnerabilidades.	Identificación y seguimiento a la solución de vulnerabilidades.	Equipo de seguridad	- Riesgo Acceso Ilegal.

#	Actividad	Descripción	Resp. Principal	Riesgo o requerimiento asociado
				- Riesgo Manipulación indebida de la información para beneficio personal o de terceros.
5.	Mejora de la gestión del acceso.	Identificación de brechas y posterior mejora de la gestión de acceso e identidades.	Equipo de seguridad	- Riesgo Acceso Ilegal. - Riesgo Manipulación indebida de la información para beneficio personal o de terceros.
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.	Equipo de seguridad	Riesgo Interrupción de los servicios TIC por problemas asociados a la plataforma tecnológica.
7.	Sensibilización en Seguridad de la Información.	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.	Equipo de seguridad	Riesgo Acceso Ilegal.
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.	Equipo de seguridad	REQ4. Mejorar la seguridad tecnológica.

Tabla 3 - Plan de Tratamiento de Riesgos de Seguridad de la Información