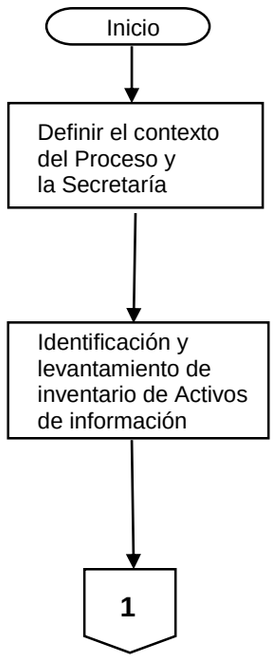
PROCESO	Tecnologías de la Información y las comunicaciones	**SECRETARIA U OFICINA**	**Secretaría de TIC**
PROCEDIMIENTO	Gestión de Riesgos de Seguridad Digital		
OBJETIVO	Establecer el procedimiento para la identificación, análisis y gestión de riesgos de seguridad digital.		
ALCANCE	El procedimiento inicia con la identificación de activos de información, después de hacer una identificación de riesgos y controles asociados a dichos activos, termina con el plan de tratamiento de riesgos de seguridad digital, es aplicable a todos los procesos y sus áreas que conforman el sistema integrado de gestión de la Gobernación de Santander.		

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	Identificar el contexto interno y externo del proceso y el área responsable	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Formato contexto estratégico diligenciado	Formato para la formulación del contexto interno y externo (ES-SIG-RG-142) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)
	Identificar y valorar los activos de información pertenecientes a cada uno de los procesos y áreas responsables Diligenciar el formato inventario de activos de Información con la información característica de cada activo	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Formato activos de información diligenciado	Inventario Activos de Información (AP-TIC-RG-19) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	Identificar los riesgos inherentes asociados a los activos de información identificados Identificar amenazas y vulnerabilidades asociadas a los activos de información identificados	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Mapa de riesgos de Gestión y Seguridad Digital diligenciado	Mapa de riesgos de gestión y seguridad digital (ES-SIG-RG-14) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)
	Valorar la probabilidad e impacto de los riesgos identificados	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Mapa de riesgos de Gestión y Seguridad Digital diligenciado	Mapa de riesgos de gestión y seguridad digital (ES-SIG-RG-14) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)
	Identificar los controles existentes y valorar su eficacia y eficiencia	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Mapa de riesgos de Gestión y Seguridad Digital diligenciado	Mapa de riesgos de gestión y seguridad digital (ES-SIG-RG-14) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)

FLUJOGRAMA	ACTIVIDADES	RESPONSABLES		PUNTOS DE CONTROL	REGISTROS
[No] [Nombre de la Actividad]	[Descripción de la Actividad]	AREA	CARGO		[Documento] [Código]
	Definir el plan de tratamiento de riesgos en respuesta al riesgo residual	Cada una de las Secretarias	Funcionario Designado (Responsable del proceso)	Mapa de riesgos de Gestión y Seguridad Digital diligenciado	Mapa de riesgos de gestión y seguridad digital (ES-SIG-RG-14) Guía metodológica para la gestión de riesgos de seguridad digital (AP-TIC-GI-01)

SALIDA DE LA ACTIVIDAD	Inventario de Activos de Información Mapa de Riesgos de Seguridad Digital Plan de Tratamiento de Riesgos de Seguridad Digital
DEFINICIONES	**Activo de información:** Es la información que, por su importancia para las actividades de la Gobernación de Santander, es reconocida como un bien que tiene un valor significativo para la Entidad. En el contexto de la norma ISO/IEC 27001 son: “Conocimientos, datos o información que una organización o entidad valora y por lo tanto debe proteger”, esta puede existir de forma física (archivos impresos, libros, Cd’s, etc) o lógica (Bases de datos, archivos en Word, Excel Pdf, fotografías, videos, etc). **Amenaza:** [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

	Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada, cuando ésta así lo requiera. **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos **ISO 27001:2013:** norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. **ISO 27005:** Estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. **Modelo de Seguridad y Privacidad de la información (MSPI):** Documento del MINTIC con los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado. **Riesgo:** [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
OBSERVACIONES	El presente procedimiento esta soportado con la guía metodológica para la gestión de riesgos de seguridad digital: (http://historico.santander.gov.co/intra/index.php/sig/finish/594-4-manuales-instructivos-guias-planes-politicas-reglamentos/11908-guia-metodologica-para-la-gestion-de-riesgos-de-seguridad-digital) El presente procedimiento cuenta con una herramienta para la identificación y valoración de los activos de información: (http://historico.santander.gov.co/intra/index.php/sig/viewdownload/593-3-formatos/11972-inventarios-de-activos-de-informacion) El presente procedimiento cuenta con una herramienta para la identificación y valoración de los riesgos: (http://historico.santander.gov.co/intra/index.php/sig/viewdownload/581-3-formatos/12405-mapa-de-riesgos-de-gestion-y-seguridad-digital)

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	REVISÓ	APROBÓ
0	27/09/2021	Creación del Procedimiento de Gestión de Riesgos de Seguridad Digital	**EDWIN ORLANDO CORREA** Director de Sistemas de Información	**RICARDO FLOREZ RUEDA** Secretario de TIC