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

Corporación Autónoma Regional de Santander

www.cas.gov.co

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos tiene como objetivo mitigar los riesgos frente a un análisis de vulnerabilidades donde pretende cumplir con los principios de la seguridad de la información como lo son: Confidencialidad, integridad y disponibilidad de la información.

El Plan define unos riesgos identificados por la entidad, el cual se establecen controles que permiten definir unas actividades con responsables para lograr mitigar el riesgo y no se materialice.

Las actividades se definieron teniendo en cuenta la información del análisis de riesgos, de las necesidades y el contexto de los procesos de la entidad en cuanto a la seguridad y privacidad de la información proporcionando las herramientas necesarias para identificar sus características y definir los pasos a seguir para su ejecución.

OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas establecidas a nivel Nacional.

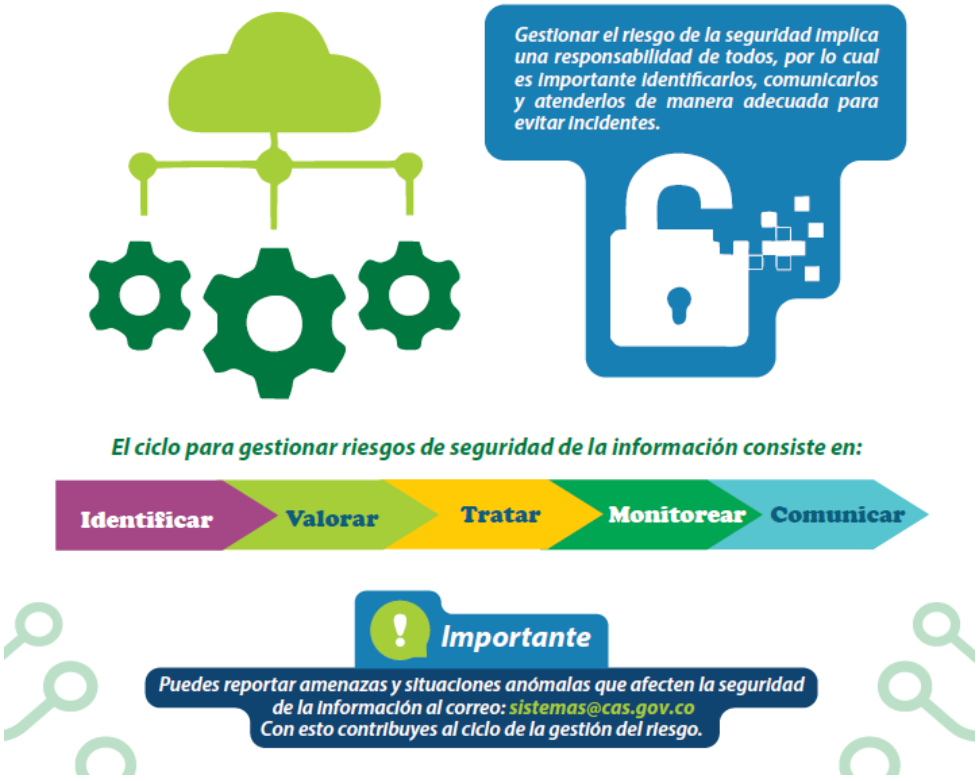
- Definir y aplicar los controles para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, preservando los principios de Confidencialidad, Disponibilidad e Integridad de la información.

- Realizar proceso de Sensibilización de la política de Seguridad de la Información de la información, con el fin de fortalecer conocimientos del uso de las herramientas tecnológicas.

ALCANCE

Es la estrategia para combatir las amenazas del mundo digital, también conocida como seguridad digital. Con el aumento de las tecnologías y la conectividad de nuevos dispositivos, la seguridad de la información evoluciona y debe ver nuevos retos del ciberespacio, es decir es ese lugar que no es físico, donde interactuamos mediante nuestras redes, programas y accesos.

- **GESTION DE RIESGOS DE SEGURIDAD**



- **PRINCIPIOS**


Confidencialidad
Significa que la información sea solo accesible para las personas, procesos o entidades autorizadas.
Principios de la Seguridad de la Información
101011 00
11 00 111 0
01 0000111
10 0 0 11100
0 0 1 01 01 0
Disponibilidad
Garantiza que la información sea accesible cuando se requiere y donde se necesita.
Integridad
Para que la información sea útil y genere valor esta no debe ser modificada, a menos que se requiera, y así mantener su veracidad.

La identificación de los activos de la información es uno de los principales pasos para garantizar la seguridad de los mismos, estos pueden ser físicos como edificios, archivos, servidores, equipos, etc. o digitales como aplicaciones, datos y servicios. La información debe ser siempre clasificada y resguardada de acuerdo a dicha evaluación.

METODOLOGIA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2024					
ítem	**Control**	**ítem-control**	**Aplica**	**Descripción**	**Responsable de ejecución**
1	Políticas para la seguridad de la información	Políticas para la seguridad de la información	Si	M-PGT-001-manual-de-politicas-de-seguridad-de-la-informacion v 4.0	OFICINA GIT
2	Revisión de las políticas para seguridad de la información	Revisión de las políticas para seguridad de la información	Si	Definido según aprobación del comité de gestión institucional	OFICINA GIT
3	Roles y responsabilidades para la seguridad de información	Roles y responsabilidades para la seguridad de información	Si	Delegados por comité institucional a la oficina de GIT CAS	OFICINA GIT
4	Seguridad de la información en la gestión de proyectos	Seguridad de la información en la gestión de proyectos	SI	Se debe incluir en los proyectos a ejecutar evaluaciones de seguridad de la información de acuerdo con los temas o activos a tratar en la entidad.	OFICINA GIT
5	Política para dispositivos móviles	Políticas para la seguridad de la información	Si	Se debe realizar denegación de servicio acceso streaming	OFICINA GIT
6	Toma de conciencia, educación y formación en la seguridad de la información	Toma de conciencia, educación y formación en la seguridad de la información	Si	Se debe construir el plan de sensibilización y toma de conciencia de la seguridad digital, así como la socialización de acciones y políticas para fortalecer la cultura corporativa de seguridad digital.	OFICINA GIT
7	Inventario de activos	Inventario de activos	Si	Se construirá el inventario de activos y socializará con cada área que aprobará su gestión y pertenencia de activos tanto tecnológicos como documentales.	OFICINA GIT
8	Clasificación de la información	Clasificación de la información	Si	Se cumple de acuerdo con la ley 1712 2014	OFICINA GIT
9	Política de control de acceso	Política de control de acceso	Si	Sensibilización Protocolo de control de acceso	OFICINA GIT
10	Política sobre el uso de los servicios de red	Política sobre el uso de los servicios de red	SI	Se construirá y socializará las instrucciones para la gestión de activos a nivel de usuario final y	OFICINA GIT

				las recomendaciones de su buen uso.	
11	Registro y cancelación del registro de usuarios	Registro y cancelación del registro de usuarios	Si	Revisión de usuarios en el registro y cancelación.	OFICINA GIT
12	Suministro de acceso de usuarios	Suministro de acceso de usuarios	Si	Solicitud por medio del Formato de Servicios TICs.	OFICINA GIT
13	Gestión de información de autenticación secreta de usuarios	Gestión de información de autenticación secreta de usuarios	Si	Protocolo de control de acceso y política de Seguridad de la Información.	OFICINA GIT
14	Revisión de los derechos de acceso de usuarios	Revisión de los derechos de acceso de usuarios	Si	Protocolo de control de acceso y política de Seguridad de la Información.	OFICINA GIT
15	Retiro o ajuste de los derechos de acceso	Retiro o ajuste de los derechos de acceso	Si	Protocolo de control de acceso y política de Seguridad de la Información.	OFICINA GIT
16	Restricción de acceso Información	Restricción de acceso Información	Si	Protocolo de control de acceso y política de Seguridad de la Información.	OFICINA GIT
17	Sistema de gestión de contraseñas	Sistema de gestión de contraseñas	Si	Procedimiento de Gestión de contraseñas	OFICINA GIT
18	Perímetro de seguridad física	Perímetro de seguridad física	Si	Sí contamos con un centro de datos y áreas de contabilidad con operaciones sensibles, pero No tenemos áreas de procesamiento de archivos confidenciales	OFICINA GIT
19	Protección contra amenazas externas y ambientales	Protección contra amenazas externas y ambientales	SI	Se cuenta con controles de temperaturas en el centro de datos, extintores y medidas de precauciones para inundaciones	OFICINA GIT
20	Trabajo en áreas seguras	Trabajo en áreas seguras	Si	Se tiene el Procedimiento para la Identificación de peligros y Riesgos	OFICINA GIT
21	Ubicación y protección de los equipos	Ubicación y protección de los equipos	SI	Los equipos de escritorio tienen los controles para evitar este tipo de accidentes, así como se cuentan con pólizas que cubren los equipos informáticos, el centro de datos cumple también con las normas	OFICINA GIT
22	Mantenimiento de equipos	Mantenimiento de equipos	Si	Se realizan mantenimientos a equipos propios de la CAS	OFICINA GIT
23	Respaldo de información	Respaldo de información	Si	Las copias de seguridad y la herramienta en Veeam backup, se realiza todos los días backup de los servidores en producción	OFICINA GIT
24	Instalación de software en sistemas operativos	Instalación de software en sistemas operativos	Si	Políticas de Seguridad de la Información	OFICINA GIT
25	Gestión de las vulnerabilidades técnicas	Gestión de las vulnerabilidades técnicas	Si	Realizar análisis de vulnerabilidades, aplicar políticas de Seguridad de la Información	OFICINA GIT

26	Restricciones sobre la instalación de software	Restricciones sobre la instalación de software	Si	Políticas de Seguridad de la Información	OFICINA GIT
27	Políticas y procedimientos de transferencia de información	Políticas y procedimientos de transferencia de información	Si	Acuerdo de confidencialidad	OFICINA GIT
28	Mensajería electrónica	Mensajería electrónica	Si	Se asignan correos electrónicos mediante solicitud firmada por jefe de oficina y el solicitante, Si se usan certificados SSL y el proveedor de hosting protege mediante firewall el envío y recepción de correos	OFICINA GIT
29	Acuerdos de confidencialidad o de no divulgación	Acuerdos de confidencialidad o de no divulgación	Si	Se cuenta con el Acuerdo de Confidencialidad para todos los funcionarios y contratistas	OFICINA GIT
30	Identificación de la legislación aplicable y de los requisitos contractuales	Identificación de la legislación aplicable y de los requisitos contractuales	Si	El área jurídica evaluara los riesgos legales y matrices de cumplimiento además de evaluar y aportar el respectivo normograma institucional para su funcionamiento acorde la legislación vigente.	OFICINA GIT
31	Derechos de propiedad intelectual	Derechos de propiedad	Si	Los contratos incluyen cláusulas de protección al trabajo realizado y propiedad intelectual	OFICINA GIT
32	Privacidad y protección de datos personales	Privacidad y protección de datos personales	Si	Actualmente se tiene la política de protección de datos personales publicada y socializada en sitios web e Intranet de la CAS	OFICINA GIT
33	Reglamentación de controles criptográficos	Reglamentación de controles criptográficos	Si	Se evaluará los controles y reglamentos pertinentes de acuerdo con los sistemas, proyecto u otras iniciativas que requiera proteger la información con algoritmos criptográficos.	OFICINA GIT
34	Revisión del cumplimiento técnico	Revisión del cumplimiento técnico	Si	El área TIC evaluara regularmente los controles existentes con el fin de endurecer e identificar adecuadamente los controles pertinentes para la seguridad Digital.	OFICINA GIT