PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DE SANTANDER

CAS

2023

Introducción

La seguridad de la información es uno de los retos más grandes para la siguiente década y en escenario colombiano reciente crece el interés en tener capacidades y habilidades para salvaguardar la información de las entidades y personas, además de garantizar derechos como la privacidad que cada vez toman una relevancia crucial en el uso de la tecnología.

Las definiciones de gobierno digital propuesta por el MINTIC y la responsabilidad de gestión un enfoque de riesgos hace que las entidades se deban preparar y planear acciones para generar confianza digital dentro sus servicios internos y externo donde prima el interés común, por lo tanto, es vital velar por capacidades que se deban robustecer, fortalecer e invertir para esta finalidad. Estival para la corporación autónoma regional de Santander primar sus escenarios de protección de la información bajo las siguientes aristas:

- Gestión de usuarios y privilegios
- Gestión de vulnerabilidades y malware
- Gestión de la mejora continua de la seguridad de la información
- Gestión de la seguridad en la infraestructura y aplicaciones
- Gestión de las habilidades de seguridad de la información y sensibilización

1. Gestión de usuarios y privilegios

La gestión de usuarios es fundamental para garantizar la seguridad desde el punto de vista de la confidencialidad e integridad de los datos, esto significa que la CAS deberá evaluar y garantizar el correcto uso de accesos mediante claves y contraseñas a los diferentes sistemas de información, aplicaciones e infraestructuras. Por lo tanto, se deberá revisar:

- GUP.1 Revisión de usuarios asignados en sistemas de información (SIG, correo, financiero, etc)

- GUP. 2 aprobación de usuarios existentes por cada jefe de oficina y áreas de la CAS.

Estas acciones se realizarán en dos ocasiones al año.

2. Gestión de las vulnerabilidades y malware

Se debe evaluar las aplicaciones y sistemas de información expuesto con software de gestión de vulnerabilidades como ZAP-OWASP, para buscar vulnerabilidades sobre aplicaciones desplegadas de manera interna y externa como son, el sitio web, sistema de información geográfico, SIHR, etc. Adicionalmente se debe evaluar constantemente las alertas de los agentes de antivirus y evaluar contra el inventario de equipos existentes para garantizar la cobertura sobre la infraestructura y redes de la corporación.

-GVM.1 gestión de vulnerabilidades – I cuatrimestre

-GVM.2 gestión de vulnerabilidades – II cuatrimestre

-GVM.3 gestión de vulnerabilidades – III cuatrimestre

-GVM.4 Revisión de consola antivirus -I semestre

-GVM.5 Revisión de consola antivirus -II semestre

3. Gestión de la mejora continua de la seguridad de la información

En la gestión continua de la seguridad se debe evaluar y robustecer la matriz documental creando los procedimientos pertinentes del proceso de gestión de seguridad de la información apalancados dentro del proceso de gestión de la información y tecnologías de apoyo – GIT. Se deberán construir los siguientes documentos:

- **GCON.1 Creación de procedimiento de gestión de vulnerabilidades**
- **GCON.2 Creación de procedimiento de gestión de incidentes**
- **GCON.3 Creación de procedimiento de gestión de continuidad**
- **GCON.4 Creación de procedimiento de gestión de respaldo y recuperación**
- **GCON.5 Actualización de manual de seguridad y privacidad**
- **GCON.6 revisión de política de seguridad de la información**
- **GCON.7 Auditoría interna de seguridad de la información**

4. Gestión de la seguridad en infraestructuras y aplicaciones

Dentro de esta capacidad se enfocará en el acompañamiento de acciones de despliegue de infraestructuras nuevas y tecnologías para garantizar el correcto funcionamiento de tecnologías de la información. Esto incluye:

- **GINF.1 Acompañamiento despliegue de correo electrónico**
- **GINF.2 Acompañamiento a despliegue de infraestructuras de redes.**
- **GINF.3 Evaluación de sistemas existentes de inventario de activos y software de mesa de servicio.**
- **GINF.4 Diseño de proyecto de herramienta para gestión de dominio y directorio activo.**

5. Gestión de las habilidades enfocadas en seguridad de la información y sensibilización de usuarios.

La seguridad de la información debe contemplar la concienciación de usuarios a cualquier nivel desde los roles administrativos y técnicos, tomar conciencia y ser sensibles que las acciones mínimas pueden desencadenar grandes eventos de seguridad y por lo cual crear cultura es fundamental para una sana convivencia de los entornos digitales seguros y confiables.

- **GHS.1 Sensibilización de seguridad y privacidad – I trimestre**
- **GHS.2 Sensibilización de seguridad y privacidad – II trimestre**
- **GHS.3 Sensibilización de seguridad y privacidad – III trimestre**
- **GHS.4 Sensibilización de seguridad y privacidad – IV trimestre**
- **GHS.5 Capacitaciones roles técnicos CAS – I semestre**
- **GHS.6 Capacitaciones roles técnicos CAS – II semestre**