PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORACIÓN

Aprobó
SANDRA QUIROZ VILLA
Gerente

Elaboró
JUAN CARLOS GIRALDO CHARRY
Coordinador de Comunicaciones

ENERO 2025

Contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información es importante para las personas, naturales y/o jurídicas; con base en ella se toman a diario, decisiones en todos los entornos. Es por ello que se debe tener la seguridad y la garantía de que es, actual y veraz.

La tecnología por su parte se convierte en el mejor vehículo para que la información fluya constantemente y pueda ser útil, en los momentos que así se determine.

Los procesos de una entidad están compuestos básicamente por información. Y la tecnología le agrega valor a ese activo, haciéndolo más fundamental en la toma de decisiones.

La dependencia de la entidad de este binomio (información – tecnología), obliga a que dicho activo sea considerado de alto riesgo, por su valor intrínseco, por lo que se hace necesario construir lineamientos y poner en prácticas, normas que controlen y minimicen los riesgos y su impacto en la entidad.

Esos lineamientos y normas deben permitir el control y administración efectiva de los datos, debido en parte a que en la ejecución de actividades se verá incrementado, la exposición y vulnerabilidad de las TICS:

- Ataques a través de software malicioso o virus informáticos.
- Ataque de intrusión.
- Ingreso de correos no deseado con contenido malicioso (correo fraudulento).
- Uso de claves de acceso a la red sin la consciencia de su confidencialidad.
- Instalación de software no institucional y/o no licenciado.
- Pérdida de información crítica de la entidad.
- Manejo de memorias USB con información confidencial o critica de la entidad.
- Accidente o desastre que interrumpa o degrade los servicios.
- Mal uso de los privilegios de acceso a la información o entrega de información confidencial de manera accidental o deliberada.
- El no uso del servidor corporativo para almacenar y proteger la información que comprenda el desarrollo del cargo.

El presente manual pretende contener políticas, pautas y criterios que norman el uso de la información en cualquier formato, para las partes interesadas; cumpliendo con las disposiciones legales vigentes, y con el objeto de minimizar riesgos y salvaguardar la información de la entidad.

OBJETIVO GENERAL

Suministrar y proveer a las partes interesadas de la entidad una herramienta guía que los oriente en el uso debido de la información y el adecuado manejo de las TI, controlando los riesgos en los que puede estar inmersa la entidad. Y asegurando la garantía a fin de mantener su disponibilidad, integridad y confidencialidad y el uso de las TIC de manera eficaz, eficiente y uniforme.

PRINCIPIOS

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

- Propuesta de explicar el detalle de cada principio.
- Promover comportamientos de seguridad responsables.
- Exhortar las actuaciones profesionales y técnicas.
- Promover una cultura positiva para la seguridad.
- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Promover la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.
- Proteger la organización.
- Soportar el actuar de la entidad.
- Enfocarse en la organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad.
- Concentrarse en aplicaciones organizacionales críticas.
- Buscar el desarrollo de sistemas de información de forma segura.

ROLES Y RESPONSABILIDADES ASOCIADAS A LA PRESENTE POLÍTICA

Comité de Dirección de Seguridad de la Información.

La entidad reglamentará su creación, sus funciones son:

- Formular y mantener actualizadas las políticas de seguridad de la información para toda la entidad.
- Revisar, aprobar y promover el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

Asesores, gerente, directores y profesionales con personal a cargo.

- Asegurar que los servidores públicos y contratistas bajo su responsabilidad conozcan, entiendan y atiendan las políticas contenidas en el presente manual.

- Aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad de la información dentro de los procesos del Sistema Integrado de Gestión que lideren.

Servidores públicos y contratistas externos.

- Conocer y cumplir las políticas indicadas en este manual.
- Reportar las infracciones o incumplimientos que identifique.
- Apoyar a otros servidores en el cumplimiento de las políticas indicadas en este manual