POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN.

EXTRUSIONES

1. PROPOSITO.

Establecer los lineamientos de seguridad de la información de EXTRUSIONES para las actividades relacionadas con su actividad comercial y gestionar las normas Corporativas a través de la Alta dirección para salvaguardar la Confidencialidad, Disponibilidad e Integridad de la información.

2. ALCANCE

La alta dirección aprueba esta política y la divulga en Extrusiones, con alcance a todas las unidades de negocio y partes interesadas para su debida aplicación y cumplimiento. Además, se compromete a asignar los recursos necesarios para su implementación y mejora continua.

3. METODOLOGÍA (MODELO METODOLÓGICO DE LA GESTION DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN)

En EXTRUSIONES se establece una Estructura de la Gestión de Riesgos de Seguridad y de la información, para lo cual la se ha adoptado las buenas prácticas de la norma ISO 27005 Sistema de Gestión de los riesgos de seguridad de la información. Esta norma contiene las siguientes etapas “Proceso de gestión de riesgos” así:

Establecer el Contexto del riesgo: Comprende toda la información acerca de la Empresa que es pertinente, mediante la evaluación de las condiciones del entorno (interno/externo) que podrían generar eventos que impacten de forma positiva o negativa el cumplimiento de los objetivos de los procesos.

Identificación de riesgos: El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del análisis del Contexto y debe partir de la claridad de los objetivos estratégicos de la Empresa para la obtención de resultados, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

Valoración de riesgos

Evaluación de los riesgos: Para realizar la Evaluación del Riesgo se debe tener en cuenta la posición del riesgo en la Matriz, según su grado de criticidad.

Planes de tratamiento: El tratamiento de los riesgos son las acciones encaminadas a gestionarlos con el fin de mitigarlos y controlarlos de la manera más efectiva para la Empresa.

Aceptación de los riesgos: Los líderes de procesos aceptan los niveles del riesgo y sus controles aplicables.

3.1 POLÍTICA DE SEGURIDAD CORPORATIVA

DECLARACIÓN DE LA POLÍTICA

La alta dirección de EXTRUSIONES considera la información como activo estratégico para las operaciones del negocio, por lo tanto, se compromete a apoyar las actividades necesarias para protegerla con medidas de seguridad, aumentando la confianza de las operaciones para los clientes, socios, directivos, empleados, el gobierno y las demás partes interesadas. Este compromiso incluye:

- Proteger la integridad de la información en sus procesos del negocio.
- Establecer mecanismos de disponibilidad de la información y servicios de tecnología de la información.
- Generar atributos de confidencialidad de la información en actividades, procesos y sedes del negocio.
- Generar capacidad de cumplimiento de los requisitos legales en materia de derechos de propiedad intelectual, privacidad y protección de la información de datos personales como lo requiere la legislación aplicable a la compañía.

La alta dirección demuestra este compromiso con el apoyo y suministro de los recursos necesarios para el logro de los objetivos de seguridad de la información, con la aprobación y difusión de las políticas de seguridad de la información.

Las políticas para el uso de la información y de los servicios de procesamiento se describen en el documento Manual de Políticas de Seguridad de la Información, y son aplicables a los empleados, contratistas y visitantes a las instalaciones de EXTRUSIONES, así como las partes interesadas con accesos a través de las redes disponibles.

NOTA: Las políticas y lineamientos contenidos en este documento se basan en los principios internacionalmente aceptados para seguridad de la información. Los cuales están incluidos en la norma internacional ISO 27001:2013 Sistema de gestión de seguridad de la información e ISO 27002 Código de práctica.

3.2 ALCANCE DE TIC.

La Política Corporativa de Seguridad de la información incluye los activos de información descritos:

- **Infraestructura** (Redes, comunicaciones, enlaces, data center, nube).
- **Sistemas de información:**
- **Información** (Transaccional, en movimiento, en reposo).
- **Servicios tercerizados** (proveedores de servicios de T.I.).
- **Personas** (empleados, partes interesadas, terceras partes).

3.3 CUMPLIMIENTO

Esta política hace parte del gobierno corporativo y se determina de estricto cumplimiento del alcance y la estructura Organizacional, al igual que sus roles y responsabilidades.

3.4 ROLES Y RESPONSABILIDADES:

Ver documento de Roles y responsabilidades de la seguridad de la información.

3.5 MARCO NORMATIVO Y LEGAL

El marco normativo que contempla estas políticas se enmarca en las buenas prácticas de las siguientes normas internacionales:

Norma ISO 27001:2013: especifica los requisitos para establecer, mantener y mejorar un sistema de gestión de seguridad de la información dentro del contexto de la Compañía.

NORMA ISO 27005: especifica la metodología para la gestión de los riesgos de seguridad de la información.

COBIT 5: Objetivos de seguridad de la información y la tecnología relacionada, la cual provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las T.I Corporativas, además de crear valor a las T.I.

3.6 MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Este manual se relaciona con otras que direccionan las actividades propias de EXTRUSIONES y son las aplicables a sus procesos y las características de estos, las políticas conexas descritas en este manual son las siguientes:

3.6.1 Control de acceso (norma ISO27001 numeral 9)
3.6.2 Clasificación (y manejo) de la información (norma ISO27001 numeral 8.2)
3.6.3 Seguridad física y del entorno (norma ISO27001 numeral 11)
3.6.4 Copias de respaldo (norma ISO27001 numeral 12.3)
3.6.5 Transferencia de información (norma ISO27001 numeral 13.2) *
3.6.6 Protección contra códigos maliciosos (norma ISO27001 numeral 12.2) *
3.6.7 Gestión de vulnerabilidades técnicas (norma ISO27001 numeral 12.6.1) *
3.6.8 Controles criptográficos (norma ISO27001 numeral 10) *
3.6.9 Seguridad de las redes y comunicaciones (norma ISO27001 numeral 13) *
3.6.10 Privacidad y protección de información de datos personales (norma ISO27001 numeral 18.1.4)
3.6.11 Conexión remota (norma ISO27001 numeral A 6.2.2)
3.6.12 Relaciones con los proveedores (norma ISO27001 numeral 15)
3.6.13 Mantenimiento y obsolescencia tecnológica (norma ISO27001 numeral A 11.2.4)

Políticas orientadas a los usuarios finales:

3.6.14 Uso aceptable de los activos (norma ISO27001 numeral 8.1.3)
3.6.15 Política de escritorio y pantalla limpia (norma ISO27001 numeral 11.2.9)
3.6.16 Dispositivos móviles (norma ISO27001 numeral 6.2) *
3.6.17 Restricciones sobre instalaciones y uso del software (norma ISO27001 numeral 12.6.2)
3.6.18 Teletrabajo (norma ISO27001 numeral A.6.2.2)

Estas políticas se comunican a los empleados y a las partes externas interesadas, mediante campaña de toma de conciencia, educación y formación en la seguridad de la información, según las buenas prácticas de ISO 27001 numeral 7.2.2.

Los numerales señalados con * contienen directrices enmarcados en la seguridad de la información.