POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Información del Documento

- **Organización:** Inixa
- **Fecha de Creación:** 15 de marzo de 2025
- **Versión:** 1.0

1. Introducción

Este documento establece la Política de Seguridad de la Información para Inixa, proporcionando un marco de referencia para la protección de los activos de información de la organización.

2. Objetivo

El objetivo de esta política es establecer los principios y requisitos necesarios para proteger la confidencialidad, integridad y disponibilidad de la información de Inixa, asegurando el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables.

3. Alcance

Esta política aplica a:

- Todos los empleados, contratistas y terceros que tengan acceso a los activos de información de Inixa
- Todos los sistemas de información, infraestructura y procesos dentro del alcance del SGSI
- Toda la información creada, recibida, almacenada, transmitida o procesada por Inixa, independientemente de su formato o medio

4. Principios de Seguridad de la Información

4.1 Confidencialidad

La información debe ser accesible únicamente para aquellos que están autorizados a acceder a ella.

4.2 Integridad

La exactitud y completitud de la información deben ser salvaguardadas.

4.3 Disponibilidad

La información debe estar disponible para los usuarios autorizados cuando sea requerida.

5. Roles y Responsabilidades

5.1 Alta Dirección

- Aprobar la Política de Seguridad de la Información
- Asignar recursos para la implementación y mantenimiento del SGSI
- Revisar periódicamente la eficacia del SGSI

5.2 Responsable de Seguridad de la Información

- Desarrollar, implementar y mantener el SGSI
- Coordinar actividades de seguridad de la información
- Reportar a la alta dirección sobre el desempeño del SGSI

5.3 Responsables de Departamentos

- Implementar los controles de seguridad en sus áreas de responsabilidad
- Fomentar la concienciación en seguridad de la información

5.4 Empleados, Contratistas y Terceros

- Cumplir con las políticas y procedimientos de seguridad
- Reportar incidentes de seguridad
- Proteger los activos de información a los que tengan acceso

6. Políticas Específicas

6.1 Control de Acceso

- El acceso a la información debe estar basado en los principios de mínimo privilegio y necesidad de conocer
- Todos los usuarios deben tener identificaciones únicas
- Las contraseñas deben cumplir con requisitos mínimos de complejidad
- Los accesos privilegiados deben ser estrictamente controlados

6.2 Seguridad Física y Ambiental

- Las áreas que contienen información sensible deben estar protegidas con controles de acceso físico
- Los equipos deben ser protegidos contra amenazas físicas y ambientales

6.3 Seguridad de Operaciones

- Los sistemas operativos deben mantenerse actualizados y protegidos
- Se debe implementar protección contra malware
- Se deben realizar copias de seguridad regulares

6.4 Seguridad de las Comunicaciones

- Las redes deben ser segmentadas y protegidas
- La información en tránsito debe ser cifrada cuando sea necesario
- Las transferencias de información deben estar sujetas a acuerdos formales

6.5 Adquisición, Desarrollo y Mantenimiento de Sistemas

- Los requisitos de seguridad deben ser incluidos en los nuevos sistemas
- Los datos de prueba deben ser seleccionados y protegidos cuidadosamente
- Los principios de ingeniería segura deben ser aplicados

6.6 Gestión de Incidentes

- Los incidentes de seguridad deben ser reportados y gestionados
- Las debilidades de seguridad deben ser reportadas y evaluadas
- Las lecciones aprendidas deben ser documentadas

6.7 Continuidad de Negocio

- Se deben desarrollar e implementar planes de continuidad
- Los planes deben ser probados y actualizados regularmente

6.8 Cumplimiento

- Se deben identificar y cumplir los requisitos legales, regulatorios y contractuales
- Los sistemas deben ser auditados regularmente

7. Cumplimiento y Sanciones

El incumplimiento de esta política puede resultar en acciones disciplinarias, hasta e incluyendo la terminación del empleo o contrato, y/o acciones legales.

8. Revisión de la Política

Esta política será revisada al menos una vez al año o cuando ocurran cambios significativos, para asegurar su continua idoneidad, adecuación y eficacia.

9. Aprobación

Aprobado por: Nombre: _____ Cargo: _____ Fecha: _____ Firma: _____