# Política de Seguridad de la Información de EFAGRAM

## 1. Objetivo

Esta política tiene como objetivo asegurar la confidencialidad, integridad y disponibilidad de la información relacionada con el Sistema de Gestión de Seguridad, Salud en el Trabajo y Ambiente (SG-SSTA), así como de cualquier otra información crítica gestionada por los sistemas de EFAGRAM, garantizando la protección de los datos de los empleados, contratistas y otros grupos de interés.

## 2. Alcance

Esta política aplica a todos los empleados, contratistas y subcontratistas de EFAGRAM que tengan acceso a los sistemas de información, así como a las tecnologías y datos que soportan el SG-SSTA y otras operaciones críticas de la empresa.

## 3. Principios

- **Confidencialidad**: Asegurar que la información sensible, especialmente relacionada con seguridad, salud y ambiente, esté protegida frente a accesos no autorizados.
- **Integridad**: Proteger la exactitud y completitud de la información, evitando la alteración indebida de datos.
- **Disponibilidad**: Garantizar que los sistemas y la información estén disponibles para su uso en todo momento, minimizando el impacto de fallos o incidentes.

## 4. Directrices

### 4.1 Protección de Datos Sensibles

- Toda información relacionada con la gestión de seguridad y salud en el trabajo, incluidos los registros de accidentes, evaluaciones de riesgo, auditorías y exámenes médicos, será tratada como confidencial.

- El acceso a la información estará restringido a personal autorizado según su rol dentro de la empresa. Se implementarán controles de acceso y autenticación para garantizar este principio.

### 4.2 Control de Acceso

- Los accesos a sistemas críticos se revisarán periódicamente y se mantendrán actualizados para evitar accesos innecesarios.

- El acceso temporal de contratistas o terceros estará regulado por acuerdos de confidencialidad y monitoreo de acceso.

### 4.3 Gestión de Cambios en los Sistemas

- Todo cambio en los sistemas de información que afecten el manejo de datos sensibles o la operación del SG-SSTA deberá ser aprobado por la gerencia del área de TI y auditado antes de su implementación.

- Los cambios en los sistemas deben ser previamente evaluados por su impacto en la seguridad de la información, y deberán documentarse las pruebas y aprobaciones correspondientes.

### 4.4 Respaldo y Recuperación de Datos

- Se cuenta con un **sistema de respaldo periódico** de toda la información crítica, incluidos los datos del SG-SSTA.

- Los planes de recuperación en caso de desastre incluirán procedimientos para garantizar la restauración rápida de la información y sistemas críticos.

- Se realizarán pruebas periódicas de los respaldos y del plan de recuperación para asegurar su efectividad.

### 4.5 Gestión de Incidentes de Seguridad de la Información

- Se establecerá un protocolo para el manejo de **incidentes de seguridad de la información**, que incluirá la detección, reporte, respuesta y mitigación de incidentes que afecten la confidencialidad, integridad o disponibilidad de la información del SG-SSTA.

- Los incidentes serán investigados para determinar su causa raíz, y se implementarán acciones correctivas y preventivas para evitar futuras ocurrencias.

### 4.6 Cumplimiento Normativo

- EFAGRAM se compromete a cumplir con todas las normativas locales e internacionales relacionadas con la protección de datos y la seguridad de la información, en especial con las leyes relacionadas con la protección de la información de seguridad y salud en el trabajo.

- Se realizará un seguimiento continuo de los cambios en las leyes aplicables para asegurar que los sistemas de información de EFAGRAM estén siempre en conformidad.

### 4.7 Capacitación y Concienciación

- Todos los empleados, contratistas y subcontratistas con acceso a los sistemas de información recibirán capacitación regular sobre esta política y los procedimientos de seguridad de la información.

- Se realizarán campañas de concienciación sobre la importancia de la seguridad de la información y el correcto manejo de los datos sensibles.

## 5. Responsabilidades

- **Departamento de sistemas**: Es responsable de la implementación, monitoreo y actualización de los sistemas de información y de esta política, asegurando que los controles sean efectivos y que se apliquen adecuadamente.

- **Usuarios del Sistema**: Son responsables de cumplir con esta política y reportar cualquier incidente de seguridad o sospecha de violación de la información.

- **Gerencia de EFAGRAM**: Asegura que los recursos necesarios para la implementación de esta política estén disponibles y supervisa su cumplimiento.

## 6. Revisión de la Política

Esta política será revisada al menos una vez al año o cuando sea necesario debido a cambios en los sistemas, las normativas o la estructura organizacional de EFAGRAM.

**FANNY PIEDRAHITA LÓPEZ**
**Representante legal y gerente.**