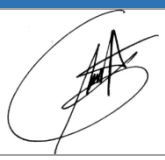
Código	PL-SI-PU-12
Versión	2.0
Publicación	30/may/2018

INFORMACIÓN PÚBLICA
Fecha de Clasificación: 24/may/2017
Páginas: en su totalidad
Fundamento Legal: Arts. 18, 19, 21 y 22 de la LFTAIPG, y 37 del RLFTAIPG
Responsable que la clasifica
Gloria Minerva González Hernández
Jefe de Seguridad de la Información

Política de equipo desatendido

Control de Versiones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Gloria Minerva González Hernández	Jefe de Seguridad de la Información	1.0	Versión preliminar del documento. Cambio de plantilla	24/may/2017	
Asley Alberto Cristales Pavón	Jefe de Capital Humano	2.0	Detalle de medidas disciplinarias, matriz de roles y responsabilidades	30/may/2018	

Control de Revisiones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Asley Alberto Cristales Pavón	Director de Operaciones	1.0		24/may/2017	

Control de Autorizaciones

Nombre	Puesto	No. Versión	Modificaciones	Fecha	Firma
Juan Carlos González Hernández	Director General	1.0		24/may/2017	

Contenido

1. Generalidades

1.1 Objetivo

Asegurar que el equipo desatendido tenga la protección apropiada; además de evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

1.2 Alcance

Todo el personal de SIFEI, ya sea interno o externo vinculado a través de contratos o acuerdos con terceros y en relación a las formas de acceso que se hayan otorgado a los usuarios sobre los activos y/o aplicaciones informáticas, cualquiera que sea la función que desempeñen.

1.3 Referencias normativas

Tabla 1. Referencias normativas y legislación vigente

Norma	Control
ISO 27001:2013	A.11.2.8 Equipo desatendido

1.4 Términos y definiciones

Tabla 2. Términos y definiciones del documento

Término	Definición
Contraseña	Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso, normalmente mediante una palabra clave.
Comité de SGSI	Comité del Sistema de Gestión de Seguridad de Información
Equipo de cómputo Corporativo	Equipo de cómputo que SIFEI proporciona a los usuarios para el desempeño de su labor.
Usuarios	Personal de SIFEI o personal externo vinculado a SIFEI.

1.5 Roles y responsabilidades

Tabla 3. Roles y responsabilidades de seguridad de la información

Actividad	Comité de Seguridad de la Información	Jefe de Seguridad de la Información	Jefe de Infraestructura	Usuarios de la información	Auditor
Definir políticas para el equipo desatendido	C A	R	C		I
Implementar la política que se describe en este documento		A	R		I
Cumplir con la política descrita en este documento en lo referente al cuidado de su información				R	I
Validar que se cumplan con las políticas de este documento	I	R			R
R – Responsable, A – Autoriza, C – Consultado, I – Informado					

2. Equipo desatendido

Un equipo desatendido es todo aquél equipo de cómputo que tiene acceso a los recursos tecnológicos de la empresa y que ha dejado de ser supervisado por el usuario al que esté asignado. Un equipo desatendido da pie al acceso de usuarios no autorizados y por lo tanto al robo y/o pérdida de información importante para la empresa. El desatender un equipo de cómputo se considera como una negligencia que se muestra hacia la obligación de cuidado de los activos. Olvidar y distraerse remiten al carácter inconsciente de tal acción.

3. Política de equipo desatendido

3.1 Responsabilidad de los usuarios de equipo desatendido

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso con contraseñas (*passwords*) y protectores de pantalla (*screensaver*) previamente instalados y autorizados por el área de Infraestructura. Para el uso adecuado de las contraseñas, se deberá consultar la Política de Uso de Contraseñas.
- Es responsabilidad de cada uno de los usuarios que cuentan con control de acceso a los equipos de información de SIFEI, proteger el equipo a los accesos no autorizados.
- Es responsabilidad de cada uno de los usuarios cuidar y velar por la protección de los datos que manejan en sus actividades diarias.
- En caso de que algún usuario se percate o sospeche de un ingreso no autorizado a su equipo, tiene la obligación de reportarlo inmediatamente a su jefe inmediato, o con algún integrante del Comité del Sistema de Seguridad de la Información.
- El acceso no autorizado de un usuario a un equipo de cómputo ajeno o a algún recurso informático no autorizado debe acreditar una sanción conforme lo señalado en el numeral 4 de este documento.

3.2 Requerimientos de seguridad para el equipo desatendido

- Todos los equipos informáticos deben pertenecer a SIFEI.
- La administración y configuración de los equipos de SIFEI debe estar a cargo por una persona asignada por la Organización.
- Todos los equipos deben contar con una contraseña de inicio de sesión.
- Todos los equipos de SIFEI deben de estar en dominio mediante Directorio Activo
    - Las reglas de dominio deben de ser administradas por una persona asignada por la Organización.
    - Debe existir una regla de dominio que indique que, a los 3 minutos de inactividad en el equipo, éste sea bloqueado de manera automática.

4. Medidas disciplinarias en caso de incumplimientos a la política

En el caso de que un colaborador de SIFEI incumpla con alguna de las políticas establecidas en el presente documento, se hará merecedor de las siguientes sanciones:

- Amonestación verbal y registro de una falta de disciplina asentándose en Acta Administrativa.

Lo anterior conforme lo señalado en el Artículo 41 del *Reglamento Interior de Trabajo*, tomándose este acto como equivalente al señalado en el numeral e) "Incumplimiento de las actividades que deban desarrollar".

En caso de que la conducta sea reiterada, se aplica lo señalado en el Artículo 25 del mismo Reglamento en lo referente a:

- Es causal de rescisión la acumulación de Actas Administrativas por falta de disciplina en el plazo allí señalado.

5. Validez y gestión de la presente política

- Este documento es válido: a partir de la fecha de publicación.
- Esta política se debe revisar con periodicidad: cada 12 meses.
- El Propietario del presente documento es: Jefe de Seguridad de la Información, quien es responsable de mantener actualizado y vigente este documento, así como asegurarse de que esté correctamente clasificado, resguardado y reservado/publicado.

6. Referencias

Nombre del Documento
Reglamento Interior de Trabajo de SIFEI.
Política de Uso de Contraseñas.