



POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE AFRI LTDA.

Pública

Políticas de Seguridad

Las políticas de Seguridad son un conjunto de normas y directrices que indican como manejar los temas de seguridad de esta institución, es un documento de alto nivel que denota el compromiso de AFRI Ltda. Con la seguridad de la información que nuestros clientes nos confían.

AFRI Ltda.
info@afri.cl

**RESPONSABLES**

ELABORADO POR:	REVISADO POR:	APROBADO POR
Gerencia de Seguridad	Comité de Seguridad	Gerente General

HISTORIAL DE CAMBIOS

NOMBRE DEL DOCUMENTO	VERSIÓN	DETALLE DEL CAMBIO	FECHA
Políticas de Seguridad de AFRI Ltda.	1.0	Creación del documento	

CLASIFICACION DEL DOCUMENTO

NIVEL DE CRITICIDAD	NIVEL DE CONFIDENCIALIDAD
Políticas de Seguridad de AFRI Ltda.	Pública

DIFUSION

AUTOR	DIRIGIDO A:
Gerencia de Seguridad	<ul style="list-style-type: none"> • Empleados de AFRI • Clientes de AFRI • Posibles Proveedores



Introducción

Este documento refleja las disposiciones e instrucciones que indican como manejar los temas de seguridad que AFRI Ltda. aplica a sus procesos de negocios, se usan estas políticas de seguridad como herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información.

Estas políticas serán revisadas con regularidad de un año, o en el caso de que se identifiquen cambios en el negocio, su estructura, objetivos, o alguna otra consideración que pueda afectar las políticas ya descritas en este documento, con el fin de determinar que sigue siendo adecuada y ajustada a la situación actual y global en la que AFRI Ltda. se encuentre inmersa.



Políticas de Seguridad de la Información.

AFRI Ltda. ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la misión, visión y valores con que AFRI Ltda. maneja la protección de sus activos de información:

- 1.- Existirá un encargado de Seguridad que será el responsable de verificar el cumplimiento de estas políticas, y asignar un Comité de Seguridad de la información que ponga en práctica estas políticas.
- 2.- Se deben definir, identificar y clasificar los activos de información de AFRI Ltda. de manera de establecer los mecanismos que serán usados para la protección de la información.
- 3.- Se deben generar controles de para proteger a la institución de violaciones de autenticación, accesos no controlados o la pérdida de integridad.
- 4.- Todos los colaboradores de AFRI Ltda. y/o posibles proveedores, tienen la responsabilidad de proteger la información a la que puedan tener acceso, y así evitar el uso indebido de la misma.
- 5.- Se realizarán auditorías internas y controles de seguimiento y cumplimiento de estas políticas, y/o la modificación de las mismas en caso de ser necesario.
- 6.- Los colaboradores de AFRI Ltda. y sus posibles proveedores tendrán la responsabilidad de reportar los incidentes de seguridad, eventos sospechosos o mal uso de los recursos que pueden ser identificados.
- 7.- Los fallos en las Políticas y/o Controles de Seguridad, deben ser reportados, registradas y monitoreadas, además de controladas.
- 8.- Se debe contar con un Plan de Contingencia que asegure la continuidad de los servicios prestados por AFRI Ltda. ante la posibilidad de eventos no controlados, incluidos desastres naturales.



9.- Acuerdos de Confidencialidad

9.1- Todos los colaboradores de AFRI Ltda. y/o posibles proveedores deben aceptar los acuerdos de confidencialidad definidos, en todo lo relativo a la confidencialidad, buen uso y protección de la información.

9.2- Cada colaborador y/o posible proveedor debe firmar individualmente un anexo de contrato o la inclusión de esta cláusula en el contrato.

10.- Documentación

10.1- La documentación digital o física debe ser clasificada por nivel de confidencialidad y sólo tendrán acceso a ella los involucrados en dicho proyecto y la gerencia de seguridad.

10.2- La documentación cargada en un repositorio tendrá privilegios de usuario de acuerdo a su nivel de confidencialidad.

11.- Acceso a Internet

11.1- No está permitido el acceso a sitios relacionados con pornografía de ningún tipo, drogas, hacking o cualquier página que tenga conflictos con la moral, ética o pueda de alguna forma ser ilegal.

11.2- No está permitido que los colaboradores u otros intercambien información de propiedad de AFRI Ltda., de sus funcionarios o de sus clientes, con cualquier persona y/o institución ajena.

11.3- No está permitida la descarga o instalación de cualquier software sin la autorización respectiva del encargado de Seguridad y/o del Comité de Seguridad.

11.4- No está permitido que los colaboradores y/o posibles proveedores escriban a través de redes sociales o internet en general a nombre de AFRI Ltda. a menos que esté autorizado por la Gerencia.

11.5- Se permite el uso de internet, siempre que cumpla con lo descrito anteriormente y que no afecte la productividad ni la seguridad de la información de AFRI Ltda. o sus clientes.



12.- Correo Electrónico:

12.1- Los colaboradores de AFRI Ltda. tendrán un correo institucional, el que será proporcionado por los administradores de correos de Afri Ltda.

12.2.- El contenido del buzón de correo electrónico, es propiedad de Afri Ltda. y de cada usuario, se debe mantener solo mensajes relacionados con trabajo.

12.3- No se permite:

- Envío de cadenas, mensajes de tipo (religioso, deportivo, político, ni mensajes que puedan resultar ofensivos de alguna manera)
- Usar el correo institucional para registros de sitios ilegales, de citas, de comunidades sociales u otros que no tengan relación con el trabajo.