

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

plbrasil
MAKES IT EASY

Política exterior - clientes

Política de seguridad de la información

Objetivo

La Política de Seguridad de la Información es una declaración formal del **Grupo PLBrasil** sobre su compromiso con la protección de la información de su propiedad y/o bajo su custodia, y debe ser cumplida por todos sus miembros y socios comerciales.

Alcance

Esta política se aplica a todos los miembros, socios comerciales, socios, gerentes, coordinadores, proveedores de servicios, consultores, auditores, socios temporales, diversos y otros socios contratados que están al servicio del **Grupo PLBrasil**.

Directrices

Según la definición de **NBR ISO/IEC 17799: 2005**, la información es un activo que, como cualquier otro activo importante para el negocio, tiene un valor para la organización y, en consecuencia, debe protegerse adecuadamente.

La Política de Seguridad de la Información tiene por objeto proteger la información de diversos tipos de amenazas, garantizar la continuidad del negocio minimizando los daños y maximizando el retorno de las inversiones y las oportunidades de negocio.

Con este fin, garantizamos el uso de software genuino y con licencia, y está prohibido el uso de programas pirateados en nuestro grupo empresarial.

La seguridad de la información se caracteriza aquí por la preservación de:

- A. **Confidencialidad**, que es la garantía de que la información es accesible sólo para las personas con acceso autorizado;
- B. **Integridad**, que es la salvaguardia de la exactitud e integridad de los métodos de información y procesamiento;

C. **Disponibilidad**, da **Política de Seguridad de la Información** se divulgará a todos los empleados y se organizará de manera que su contenido pueda ser consultado en cualquier momento.

Para garantizar estos tres elementos mencionados, la información debe ser manejada y protegida adecuadamente contra robos, fraudes, espionaje, pérdida involuntaria, accidentes y otras amenazas.

Es fundamental para la protección y protección de la información que los usuarios tomen en la acción de **Comportamiento Seguro** y sean coherentes con el objetivo de protección de la información, y deben asumir actitudes proactivas y comprometidas con respecto a la protección de la información.

Para ello, el **Grupo PLBrasil** tiene una **Política de Seguridad de la Información Interna** revisada y aprobada periódicamente por los Socios de la Compañía. Se llevan a cabo campañas continuas de sensibilización sobre seguridad de la información para difundir y supervisar la aplicación de las prácticas descritas en la política por los miembros y asociados.

La **Política de Seguridad de la Información Interna** del **Grupo PLBrasil** define y monitorea la aplicación de los siguientes elementos de seguridad:

- Sensibilización y capacitación de los miembros sobre los procedimientos de seguridad, así como el uso correcto de los activos, con el fin de reducir los posibles riesgos;
- Firma obligatoria de términos de confidencialidad por parte de miembros, clientes y socios comerciales;
- Gestión del acceso físico a las instalaciones del **Grupo PLBrasil**, incluida la inclusión, el mantenimiento y la exclusión; y
- Gestión del acceso lógico a los sistemas e información en el **Grupo PLBrasil**, incluyendo inclusión, mantenimiento y exclusión:
 - Las contraseñas se enmascaran/cifran cuando se introducen. En caso de compromiso del sistema o contraseña, el usuario está bloqueado;
 - La contraseña para el acceso al ordenador es única y personal, siendo el primer acceso realizado con la ayuda del departamento de TI, verbalmente;
 - Los usuarios validan el acceso en el momento de la entrega de contraseñas y en caso de olvido de contraseñas, el departamento de TI debe realizar una nueva creación;

- Ninguno de los proveedores establece contraseñas de acceso; todas las contraseñas, incluidas las contraseñas de software, son establecidas por el departamento de TI;
 - No hay contraseñas temporales ni directivas temporales de contraseñas;
 - Las contraseñas no caducan automáticamente. El cambio de contraseña debe ser solicitado únicamente por el usuario, directamente desde el departamento de TI.
- Gestión del acceso a certificados digitales en poder del **Grupo PLBrasil**, ya sea de sus socios o de clientes.
 - Adopción de prácticas de seguridad de la información tales como copia de seguridad diaria, autenticación y cuidado de contraseñas, restricción del acceso al correo electrónico, red interna y sitios web externos, instalación y uso de software y equipo.
 - Clasificación de información en **Grupo PLBrasil**.
 - Tratamiento de incidentes de seguridad de la información en **Grupo PLBrasil**.
 - Cumplimiento de la **Ley de Protección de Datos personales (LGPD)**.
 - Bloqueo de unidades extraíbles como flashdrives, discos externos y teléfonos móviles.

La red tiene directivas de restricción de acceso, que impiden la creación de documentos en ubicaciones informáticas comunes, como documentos de carpeta, escritorio, imágenes, etc. y, en consecuencia, hace que los usuarios almacenen los documentos en las carpetas de red (servidor). La carpeta de descargas de equipos tiene una directiva que elimina todos los archivos contenidos en ella cuando se inicia el equipo.

La red tiene directivas de bloqueo de inactividad del equipo. Después de 5 minutos de inactividad, la estación de trabajo se bloquea automáticamente.



Comité de Seguridad información

El **Grupo PLBrasil** también cuenta con un **Comité de Seguridad de la Información**, que cuenta con la participación de miembros de la alta dirección en su composición, con el objetivo de:

- Aprobar cualquier cambio en los procedimientos internos relacionados con la seguridad de la información.
- Evalúe la eficacia de los controles de seguridad del **Grupo PLBrasil**, así como la necesidad de su cambio.
- Evaluar posibles incidentes de seguridad ocurridos en el **Grupo PLBrasil** y acciones correctivas y preventivas deliberadas.
- Garantice la correcta concesión de licencias de toda adquisición de software y hardware para la gestión de información tecnológica de sus clientes



Cómo garantizamos la confidencialidad de nuestros datos

» 1. Servidores

Nuestros servidores están alojados en **Microsoft** y **Amazon**, que son responsables de administrar la seguridad de la información contenida en nuestra base de datos.

Acceda a las políticas de privacidad de datos de estas organizaciones a continuación:

Amazon - <https://aws.amazon.com/pt/compliance/data-privacy-faq/>

Microsoft - <https://azure.microsoft.com/pt-br/overview/trusted-cloud/privacy/>

» 2. Firewall e Proxy

Utilizamos la línea **FORTIGATE** para garantizar toda la seguridad del acceso a nuestra información. Los productos utilizados garantizan:

- Seguridad consolidada y redes para la empresa;
- Protección de alto nivel para prevenir amenazas;
- Red cableada e inalámbrica integrada para simplificar la TI;
- Hardware desarrollado para el mejor rendimiento de la industria;
- Gestión en la nube para facilitar la administración;
- Proporciona el mejor rendimiento de protección contra amenazas de la industria y latencia ultrabaja utilizando tecnología de procesador de seguridad (SPU) diseñada específicamente;
- Proporciona rendimiento y protección líderes en el sector para el tráfico cifrado con SSL;
- Tejido de seguridad; y
- Permite que los productos asociados listos para fabric y fortinet se integren de forma colaborativa y proporcionen seguridad de extremo a extremo en toda la superficie de ataque.

Acceda a la página del producto a continuación:

<https://www.fortinet.com/products/next-generation-firewall/overview.html>

» 3. Antivirus

Utilizamos **Kaspersky** line y **Endpoint** protection para nuestros dispositivos y ordenadores. Es una solución que va más allá de un simple antivirus empresarial y cubre varias capas de seguridad, además de realizar el bloqueo de dispositivos externos

Acceda a la página del producto a continuación:

<https://www.kaspersky.com.br/small-to-medium-business-security/endpoint-windows>

» 4. Canales de escucha, quejas

El **Grupo PLBrasil** apoya y alienta a los miembros, clientes y corresponsales a reportar cualquier evidencia de transgresión y violación de principios éticos, leyes y regulaciones, políticas, corrupción y mala conducta o conducta ilegal.

Con este fin, el **Grupo PLBrasil** pone el canal de informes a disposición a través de sitios web/o correos electrónicos, garantizando la confidencialidad de la queja y de las

partes involucradas.

Habrá un **Comité interno de investigación** que investigará los casos imparcialmente, investigando las pruebas y garantizando el anonimato del denunciante. Una vez que se determine la veracidad de la queja, será enviada a la Oficina Legal del **Grupo PLBrasil**, que validará el caso a través de las leyes vigentes.



Canal de Denuncia

etica@plbrasil.com.br | www.plbrasil.com.br

» 5. Política de no represalias

El **Grupo PLBrasil** promueve y garantiza un ambiente de protección contra cualquier forma de represalia contra los denunciantes, con el objetivo de crear un ambiente seguro, independiente e imparcial para aquellos que denuncien la práctica de actos de mala conducta, violación de normas y leyes o cualquier acto ilegal previsto en las políticas anticorrupción y conducta ética de la empresa



Canal de Denúncia

etica@plbrasil.com.br | www.plbrasil.com.br

+55 11 3292.5050

plbrasil
MAKES IT EASY

• SIGA A PLBRASIL •