POLÍTICAS DE CYBER SEGURIDAD

1 DE NOVIEMBRE DE 2023

APOLO LEX APOLEXSA S.A.
Desarrollado por Carlos Cordova Analista T.I.

POLÍTICA DE CIBERSEGURIDAD

Objetivo:

Garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información y los datos de **Apolo Lex Apolexsa S.A**. (en adelante la organización) frente a amenazas cibernéticas, asegurando así la protección de la información sensible de nuestros clientes, empleados y socios comerciales. Esta política tiene como objetivo establecer un marco robusto de controles de seguridad que permita prevenir, detectar, responder y recuperarse de incidentes de seguridad de manera eficaz, asegurando el cumplimiento de las normativas legales y los estándares de la industria pertinente. Busca fomentar una cultura organizacional de conciencia y responsabilidad en materia de ciberseguridad, capacitando a nuestro personal para reconocer y mitigar las amenazas cibernéticas en todas las áreas y niveles de la **organización**.

Alcance:

Esta política se aplica a todos los empleados, contratistas, consultores y terceros que accedan a los sistemas de información de la **organización**, ya sea de manera local o remota. Incluye todos los dispositivos y redes utilizados para procesar, almacenar o transmitir información propiedad de la **organización**, así como los sistemas de terceros que manejen información sensible en nombre de la **organización**. Abarca cualquier ubicación física o virtual donde se realice procesamiento de datos relacionado con las operaciones comerciales.

Todos los usuarios deben cumplir con esta política y los procedimientos asociados, que establecen los estándares mínimos de seguridad que deben ser implementados y mantenidos en todos los sistemas y recursos tecnológicos. Esto incluye la responsabilidad de proteger los datos confidenciales y personales, gestionar adecuadamente los accesos y privilegios, y cooperar activamente en la implementación de controles de seguridad y la respuesta a incidentes.

Responsabilidades:

- **Dirección:**

  Es responsabilidad de la alta dirección aprobar, comunicar y mantener esta política de ciberseguridad. Deben asignar los recursos necesarios para implementar controles de seguridad efectivos y promover una cultura organizacional que valore la seguridad de la información. Deben asegurarse de que se realicen evaluaciones periódicas de riesgos y auditorías de seguridad para mitigar y gestionar los riesgos de manera proactiva.

- **Personal de TI:**

  El equipo de TI tiene la responsabilidad de implementar y mantener controles de seguridad técnicos y administrativos adecuados. Esto incluye la configuración segura de sistemas y redes, la monitorización continua de la actividad de red y la detección de amenazas, así como la respuesta rápida y efectiva a incidentes de seguridad. Deben proporcionar soporte técnico y formación en ciberseguridad a todos los usuarios, asegurándose de que estén informados y capacitados para cumplir con las políticas y procedimientos establecidos.

- **Usuarios:**

  Todos los empleados, contratistas y terceros autorizados que accedan a los sistemas de información de la **organización** tienen la responsabilidad de cumplir con esta política y los controles de seguridad asociados. Esto implica proteger activamente la información confidencial y personal a la que tengan acceso, utilizar contraseñas seguras y autenticación multifactor cuando corresponda, y reportar cualquier incidente de seguridad o comportamiento sospechoso de inmediato al equipo de TI o al departamento designado para gestionar la seguridad de la información. Deben participar en programas regulares de formación y concienciación

en ciberseguridad para mantenerse actualizados sobre las amenazas emergentes y las mejores prácticas de seguridad.

Directrices:

1. **Acceso y Autenticación:**

   - Se implementarán medidas de autenticación fuertes, como contraseñas robustas y autenticación multifactor, para proteger el acceso a los sistemas y datos sensibles.
   - El acceso a los recursos de la **organización** se basará en el principio de mínimo privilegio, limitando los privilegios de acceso solo a aquellas funciones y datos necesarios para realizar las tareas laborales.

2. **Seguridad de la Información:**

   - Todos los datos confidenciales y personales serán clasificados y protegidos adecuadamente según su nivel de sensibilidad.
   - Para información sumamente sensible se aplicarán técnicas de cifrado para proteger la confidencialidad de la información durante el almacenamiento y la transmisión.

3. **Monitoreo y Detección:**

   - Se establecerán herramientas y procedimientos de monitoreo continuo de la red y los sistemas para detectar y responder rápidamente a actividades sospechosas o no autorizadas.
   - Se llevarán a cabo auditorías periódicas de seguridad y evaluaciones de vulnerabilidades para identificar y mitigar posibles riesgos de seguridad.

4. **Gestión de Incidentes:**

   - Se mantendrá un plan de respuesta a incidentes detallado que incluya procedimientos claros para reportar, investigar y mitigar incidentes de seguridad.

- Todos los incidentes de seguridad serán documentados y analizados para identificar lecciones aprendidas y mejorar los controles de seguridad existentes.

5. **Educación y Concienciación:**

   - Se proporcionará formación regular en ciberseguridad a todos los empleados para aumentar la conciencia sobre las amenazas cibernéticas y promover buenas prácticas de seguridad.
   - Se realizarán simulacros y pruebas de phishing periódicas para educar a los usuarios sobre cómo identificar y evitar ataques de ingeniería social.

Cumplimiento y Revisión:

- Se revisarán y actualizarán regularmente las políticas y procedimientos de ciberseguridad para asegurar su alineación con las mejores prácticas de la industria y las normativas legales vigentes.
- Se llevarán a cabo evaluaciones periódicas de cumplimiento para garantizar que todos los requisitos de seguridad sean cumplidos por todos los empleados y sistemas de la **organización**.