POLITICA DE SEGURIDAD DE LA INFORMACIÓN

PRESENCIA Colombo Suiza, en su compromiso con la seguridad de la información, establece las siguientes reglas generales para el uso de los activos de información:

1. Uso Exclusivo para Fines Laborales
Los activos de información, incluidos dispositivos, aplicaciones y datos, deben utilizarse exclusivamente para fines laborales relacionados con las actividades de la organización.

2. Protección de Información Confidencial
Se debe proteger la información confidencial y sensible de la organización, evitando su divulgación no autorizada. Esto incluye el uso de contraseñas fuertes y el cifrado de datos cuando sea necesario.

3. Acceso y Autenticación
El acceso a los activos de información debe estar limitado a los empleados autorizados. Se deben utilizar métodos de autenticación adecuados (como contraseñas, autenticación de dos factores) para garantizar la seguridad.

4. Uso Responsable de Recursos
Los empleados deben utilizar los activos de información de manera responsable y eficiente, evitando el uso excesivo de recursos como ancho de banda, almacenamiento y tiempo de procesamiento.

5. Prohibición de Instalación de Software No Autorizado
Está prohibido instalar o utilizar software no autorizado en los dispositivos de la organización. Solo se deben utilizar aplicaciones y herramientas aprobadas por el departamento de TI.

6. Mantenimiento de la Integridad de los Datos
Los empleados son responsables de mantener la integridad y precisión de los datos. Cualquier error o inconsistencia debe reportarse de inmediato a la persona correspondiente.

7. Cumplimiento de Políticas y Normativas
Todos los empleados deben cumplir con las políticas de seguridad de la información y las normativas legales aplicables. Esto incluye regulaciones como GDPR, HIPAA u otras específicas del sector.

8. Responsabilidad en el Uso de Dispositivos Móviles
Los dispositivos móviles utilizados para acceder a información corporativa deben estar protegidos con contraseñas y mecanismos de seguridad. Se deben evitar conexiones a redes públicas no seguras.

9. Devolución de Activos de Información
Al finalizar la relación laboral o cuando se cambien de puesto, los empleados deben devolver todos los activos de información (dispositivos, documentos, credenciales, etc.) en su estado original, asegurándose de eliminar toda la información personal o no relacionada.

10. Reporte de Incidentes de Seguridad
Cualquier incidente de seguridad, como pérdida, robo o uso indebido de activos de información, debe ser reportado de inmediato al departamento de TI o al responsable de seguridad de la información para su gestión y mitigación.

Estas reglas proporcionan un marco claro para el uso responsable y seguro de los activos de información dentro de la organización, protegiendo tanto a la empresa como a sus empleados.