POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

MINMETECEC CIA. LTDA.

Índice

1. Introducción

La protección de la información y la ciberseguridad son elementos fundamentales en nuestra organización, no solo para garantizar la integridad de los sistemas y datos, sino también para cumplir con las normativas vigentes, incluyendo la certificación BASC. Estas políticas han sido desarrolladas para que todo el personal de la empresa contribuya activamente a la seguridad de la información.

2. Objetivo

El presente documento tiene como objetivo establecer las políticas de seguridad informática y ciberseguridad que permitirán proteger la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas y recursos tecnológicos utilizados por la empresa.

3. Alcance

Estas políticas aplican a todo el personal de la empresa que utilice equipos de cómputo, dispositivos electrónicos, sistemas de información, o que tenga acceso a la red corporativa, servicios en la nube, y cualquier otra infraestructura tecnológica.

4. Definiciones y Abreviaturas

- ✓ **Software:** Programas y aplicaciones instalados en los sistemas informáticos.
- ✓ **Hardware:** Componentes físicos de los sistemas, como computadoras, servidores y dispositivos periféricos.
- ✓ **Seguridad de la Información:** Protección de la información almacenada o transmitida a través de sistemas computacionales.
- ✓ **Nube:** Modelo de almacenamiento y procesamiento de información a través de Internet.
- ✓ **Servidor en la nube:** Infraestructura virtual para el almacenamiento de datos proporcionada por terceros.

5. Políticas Generales de Seguridad

5.1 Seguridad Institucional

Todo nuevo empleado debe aceptar las condiciones de confidencialidad y uso adecuado de los recursos tecnológicos. Las credenciales de acceso (usuario y contraseña) son personales e intransferibles. Está prohibido compartir credenciales con terceros.

5.2 Capacitación en Seguridad Informática

Todo empleado debe recibir capacitación sobre las políticas de seguridad informática al ingresar a la empresa. La capacitación incluirá la importancia del manejo seguro de la información y las consecuencias de no cumplir con las políticas.

5.3 Sanciones

Cualquier incumplimiento de las políticas de seguridad, tales como divulgación no autorizada de información o uso indebido de los recursos tecnológicos, se considerará falta grave y podrá resultar en sanciones disciplinarias, incluyendo la terminación del contrato laboral. Además, aquellos empleados que cometan delitos informáticos serán sujetos a acciones legales.

5.4 Seguridad Física y Protección del Ambiente

Los equipos de cómputo deben ser protegidos contra riesgos como caídas, choques eléctricos y daños por líquidos. Los empleados son responsables de reportar inmediatamente cualquier situación que pueda comprometer la seguridad de los equipos o la información almacenada en ellos.

5.5 Uso de Dispositivos Extraíbles

El uso de dispositivos de almacenamiento externo como USBs o discos portátiles está restringido y debe ser aprobado por el departamento de Tecnología de la Información. Se fomentará el uso de servicios en la nube para compartir y respaldar la información de manera segura.

5.6 Licenciamiento de Software

Está prohibido instalar software no autorizado o sin licencia. El departamento de Tecnología de la Información realizará auditorías semestrales para verificar el cumplimiento de esta política.

5.7 Seguridad de la Red

Cualquier intento de acceder a la red corporativa sin autorización será considerado un ataque a la seguridad informática. El monitoreo continuo de la red permitirá detectar y prevenir actividades sospechosas.

5.8 Uso del Correo Electrónico

El correo electrónico corporativo debe utilizarse exclusivamente para fines laborales. Los empleados no deben usar cuentas de otros ni falsificar información en los correos. Toda comunicación de información confidencial debe ser encriptada.

5.9 Uso de Internet

El acceso a Internet proporcionado por la empresa está limitado a actividades laborales. El uso de Internet para actividades personales o la descarga de software sin autorización está estrictamente prohibido.

6. Acceso Lógico

6.1 Controles de Acceso Lógico

Cada usuario es responsable de las credenciales asignadas. Las credenciales no deben ser compartidas ni divulgadas, y se deben emplear mecanismos de autenticación seguros antes de acceder a los recursos tecnológicos de la empresa.

6.2 Administración y Uso de Contraseñas

Las contraseñas deben cambiarse cada 90 días y cumplir con los requisitos mínimos de seguridad (al menos 8 caracteres, uso de mayúsculas, minúsculas, números y símbolos). El uso compartido de contraseñas está prohibido.

6.3 Control de Accesos Remotos

El acceso remoto a los sistemas de la empresa debe ser autorizado y controlado. Se implementarán mecanismos de seguridad, como autenticación de dos factores, para proteger los accesos remotos.

7. Seguridad y Gestión de Servicios en la Nube

7.1 Generalidades

Los datos almacenados en la nube deben estar encriptados tanto en tránsito como en reposo. Se implementará autenticación de dos factores para todos los accesos a la nube.

7.2 Respaldo de Información en la Nube

Los datos críticos serán respaldados diariamente, mientras que los datos menos críticos serán respaldados semanalmente o mensualmente según corresponda. Los respaldos se realizarán automáticamente y se almacenarán en un segundo proveedor de nube para garantizar redundancia.

7.3 Acceso y Uso de Servicios en la Nube

El acceso a los servicios en la nube debe ser autorizado. Está prohibido compartir credenciales de acceso y todos los empleados deben cumplir con las políticas de confidencialidad.

7.4 Adquisición de Servicios en la Nube

Cualquier servicio en la nube que se desee implementar debe ser aprobado por el departamento de Tecnología de la Información y evaluado en términos de seguridad y riesgos.

7.5 Monitoreo y Seguridad en la Nube

El uso de herramientas de monitoreo continuo permitirá detectar actividades sospechosas. Se realizarán pruebas de recuperación de datos cada tres meses para verificar la efectividad de los respaldos.

8. Control y Continuidad de Credenciales de Superusuarios

8.1 Gestión de Accesos y Roles

Los superusuarios tendrán privilegios limitados a lo necesario para cumplir con sus funciones, minimizando el riesgo de accesos no autorizados.

8.2 Rotación de Contraseñas de Superusuarios

Las contraseñas de superusuarios deberán ser cambiadas cada tres meses, y deben cumplir con requisitos estrictos de seguridad.

8.3 Plan de Continuidad de Credenciales

En caso de emergencia, las credenciales de superusuarios estarán respaldadas en un sistema seguro y serán accesibles solo por personal autorizado.

8.4 Política de Revisión Periódica

Se realizará una revisión trimestral de los permisos asignados a los superusuarios para garantizar que se ajusten a las necesidades operativas.

9. Cumplimiento de la Seguridad Informática

9.1 Violaciones de Seguridad Informática

Está prohibido el uso de herramientas que comprometan los controles de seguridad informática. Los empleados no deben intentar explotar vulnerabilidades, excepto cuando se realicen pruebas controladas y autorizadas por el departamento de Tecnología de la Información.

9.2 Derechos de Propiedad Intelectual

Todo sistema o aplicación desarrollada por el personal de la empresa es propiedad exclusiva de la misma.

10. Responsabilidades

Es responsabilidad de cada empleado cumplir con estas políticas. El departamento de Tecnología de la Información es responsable de implementar y supervisar las medidas de seguridad. La Gerencia General es responsable de asegurar que todos los empleados cumplan con estas políticas.

11. Revisión y Actualización de las Políticas

Estas políticas serán revisadas y actualizadas periódicamente para garantizar su efectividad y cumplimiento con las normativas vigentes.

HISTORIAL DE REVISIONES

Versión No.	Fecha	Razón del Cambio	Estado del documento
0	30/09/2024	Versión Inicial	Vigente

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ing. Patricio Pacheco	Ing. Karina Ortiz	Ing. Cristina Bravo
Director de Tecnología	Subgerente de Operaciones/SGCS	Gerente General