

POLITICAS DE INFORMATICA

ALEMED Soluciones Integrales SpA

Aprobado con fecha 11 de Marzo de 2023

INTRODUCCIÓN

Este documento describe las políticas informáticas que deben ser adoptadas en ALEMED Soluciones Integrales SpA a objeto de resguardar la seguridad, eficiencia y efectividad en el uso de los recursos tecnológicos dispuestos en la empresa.

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1.1 Acceso a la Información

Por que en ALEMED SpA entendemos que la información es el activo más importante que tenemos como empresa, hacer buen uso de ella es imprescindible y la confidencialidad es aún lo más importante.

- ✓ Los colaboradores solo podrán trabajar con la información que les compete dentro de las funciones que le han sido asignadas dentro del contrato de trabajo.
- ✓ Todos los usuarios deben utilizar credenciales o contraseñas únicas, vale decir, no deben ser compartidas con nadie.
- ✓ Las contraseñas deben ser complejas y difíciles de adivinar, vale decir, no se deben utilizar contraseñas que sean demasiado obvias y se aconseja cambiarlas cada 90 días.

1.2 Protección de Datos

- ✓ Toda la información utilizada para la gestión empresarial debe ser almacenada en las carpetas que la jefatura le asigne o le indique.
- ✓ Se recomienda realizar copias de seguridad diarias de toda la información crítica.

1.3 Uso de Dispositivos

- ✓ Solo se deben utilizar los dispositivos asignados y/o autorizados por la empresa para acceder a la información corporativa.
- ✓ Los dispositivos móviles deben contar con software de gestión de dispositivos móviles (MDM) y tener la capacidad de ser borrados remotamente en caso de pérdida o robo.

2. POLÍTICAS DE USO ACEPTABLE

2.1 Uso del Correo Electrónico

Hoy en día, el correo electrónico es una fuente muy importante de ataques asociados a ciberseguridad, por lo que el buen uso de esta herramienta debe ser de máximo cuidado. Por lo anterior, se recomienda encarecidamente velar por el cumplimiento de las siguientes recomendaciones:

- ✓ El correo electrónico corporativo debe ser utilizado exclusivamente para fines laborales.
- ✓ Está prohibido el envío de correos electrónicos con contenido inapropiado, ofensivo o ilegal.
- ✓ Se debe informar a la jefatura, directa o indirecta o con el área de informática cuando se reciba algún correo sospechoso.
- ✓ No se deben abrir archivos adjuntos de correos sospechosos, ni siquiera por curiosidad, para evitar riesgos de malware.

2.2 Uso de Internet

- ✓ El acceso a Internet debe utilizarse para actividades relacionadas con el trabajo.
- ✓ Queda prohibido el acceso a sitios web no relacionados con el trabajo, especialmente aquellos que puedan comprometer la seguridad de la red.

2.3 Uso de Software

- ✓ Solo se permite la instalación de software autorizado por la empresa, tanto en pcs u otro dispositivo corporativo, tales como, celulares, tablets, etc...
- ✓ Todo el software debe ser actualizado regularmente para garantizar la seguridad y funcionalidad.

3. POLÍTICAS DE RESPALDO Y RECUPERACIÓN

3.1 Copias de Seguridad

- ✓ Se recomienda realizar copias de seguridad diarias de toda la información crítica.
- ✓ Las copias de seguridad deben almacenarse en ubicaciones seguras y ser probadas periódicamente para asegurar su integridad y disponibilidad.

3.2 Plan de Recuperación ante Desastres

En ALEMED SpA contamos con un plan de recuperación ante desastres que detalle los procedimientos a seguir en caso de fallas graves del sistema.

- ✓ El plan es revisado y actualizado regularmente.

4. POLÍTICAS DE MANTENIMIENTO Y ACTUALIZACIÓN

4.1 Mantenimiento de Equipos

- ✓ El equipo informático es mantenido y revisado regularmente para asegurar su correcto funcionamiento.
- ✓ Las actualizaciones de hardware son planificadas y se ejecutan de manera coordinada con el usuario.

4.2 Actualizaciones de Software

- ✓ Todo el software es actualizado regularmente para asegurar la seguridad y funcionalidad.
- ✓ Las actualizaciones son gestionadas por el departamento de TI y programadas para minimizar el impacto en las operaciones.

5. POLÍTICAS DE FORMACIÓN Y CONCIENCIACIÓN

5.1 Capacitación de Empleados

- ✓ Todos los empleados reciben formación, tanto al ingreso a la empresa como de manera regular, sobre las políticas informáticas y las mejores prácticas de seguridad.
- ✓ La formación incluye cómo identificar y reportar amenazas de seguridad como el phishing o spam.

5.2 Concienciación sobre la Seguridad

Regularmente se realizarán campañas de concienciación sobre la seguridad de la información a objeto de fomentar una cultura de seguridad dentro de nuestra empresa.

6. POLÍTICAS DE CONTROL Y MONITOREO

6.1 Monitoreo de la Red

- ✓ La red corporativa es monitoreada continuamente para detectar y responder a amenazas de seguridad.
- ✓ Se utilizan sistemas de detección y prevención de intrusiones (IDS/IPS).

6.2 Auditorías de Seguridad

- ✓ Se realizan auditorías de seguridad periódicas para evaluar la efectividad de las políticas y procedimientos de seguridad.
- ✓ Las auditorías son realizadas por personal interno y externo de manera regular.

7. POLÍTICAS DE CUIDADO DEL MEDIO AMBIENTE

En ALEMED SpA estamos completamente comprometidos con el cuidado del medio ambiente es por ello que solicitamos encarecidamente a nuestros colaboradores considerar las siguientes recomendaciones:

7.1 Reducción de Papel

- ✓ Promover el uso de documentos electrónicos a objeto de reducir al mínimo el uso de papel.
- ✓ Imprimir documentos solo cuando sea absolutamente necesario y utilizar ambas caras del papel, en la medida que se pueda.

7.2 Reciclaje

- ✓ Se colocarán contenedores de reciclaje, para papel, plástico y otros materiales reciclables en lugares estratégicos.
- ✓ Fomentar la separación de residuos y el reciclaje entre los empleados.

8. POLÍTICAS DE AHORRO ENERGÉTICO

8.1 Uso Eficiente de Energía

- ✓ Apagar los equipos informáticos y otros dispositivos electrónicos al final de la jornada laboral.
- ✓ Utilizar configuraciones de ahorro de energía en computadoras y monitores.

8.2 Iluminación

- ✓ Aprovechar al máximo la luz natural y apagar las luces cuando no sean necesarias.
- ✓ Utilizar ampolletas de bajo consumo energético.

9. POLÍTICAS DE HIGIENE

9.1 Limpieza de Equipos

- ✓ Mantener limpios los equipos informáticos y las estaciones de trabajo.
- ✓ Utilizar productos de limpieza adecuados para evitar daños en los equipos.

RICHARD ALEGRIA OLIVER
REPRESENTANTE LEGAL