Política de Seguridad en la Utilización de Medios Electrónicos

1. Introducción

La seguridad de la información es un pilar fundamental para nuestra organización, garantizando la confidencialidad, integridad y disponibilidad de los datos y sistemas electrónicos utilizados en nuestras operaciones. Con base en el marco normativo de la **ISO/IEC 27001:2022**, este documento establece los principios y directrices de nuestra **Política de Seguridad en la Utilización de Medios Electrónicos** con el propósito de mitigar riesgos, prevenir incidentes y asegurar el cumplimiento de requisitos regulatorios y contractuales.

2. Objetivo y Alcance

Este documento tiene como objetivo definir las políticas y controles que rigen el uso seguro de medios electrónicos, incluyendo equipos informáticos, redes de comunicación, sistemas de almacenamiento, correo electrónico, dispositivos móviles y plataformas en la nube. La política se aplica a todos los empleados, contratistas y terceros que interactúan con los sistemas de información de la organización.

3. Principios de Seguridad

Conforme a la norma **ISO/IEC 27001:2022**, la presente política se fundamenta en los siguientes principios:

1. **Confidencialidad:** Protección de la información contra accesos no autorizados.
2. **Integridad:** Garantía de que la información y los sistemas no serán alterados de manera indebida.
3. **Disponibilidad:** Asegurar el acceso a la información y los sistemas cuando sea necesario para la operación.
4. **Legalidad:** Cumplimiento de regulaciones locales e internacionales en materia de seguridad de la información.
5. **Responsabilidad:** Definición clara de roles y responsabilidades para el cumplimiento de esta política.

4. Normas y Controles Aplicables

Para garantizar la seguridad en la utilización de medios electrónicos, la organización ha adoptado los siguientes controles de seguridad:

4.1. Control de Accesos

- Implementación de autenticación multifactor (MFA) para accesos críticos.
- Restricción de privilegios administrativos y revisión periódica de accesos.
- Políticas de contraseñas robustas y gestión segura de credenciales.

4.2. Seguridad en Comunicaciones y Almacenamiento

- Uso de cifrado en almacenamiento y transmisión de datos sensibles.
- Monitorización y auditoría del tráfico de red para detectar actividades sospechosas.
- Gestión segura de dispositivos móviles y acceso remoto mediante VPN segura.

4.3. Protección contra Amenazas Cibernéticas

- Implementación de soluciones de detección y respuesta ante incidentes (EDR).
- Políticas de seguridad para el uso de software y dispositivos USB.
- Pruebas periódicas de seguridad y análisis de vulnerabilidades esanchezhernTFM0622memo....

4.4. Concienciación y Capacitación

- Programas de formación en ciberseguridad para todo el personal.
- Simulaciones periódicas de ataques de phishing y respuesta a incidentes.
- Revisión y actualización de la política de seguridad al menos una vez al año

5. Auditoría y Cumplimiento

Esta política se auditará periódicamente a través de evaluaciones internas y externas alineadas con el estándar **ISO/IEC 27001:2022**, garantizando la mejora continua del sistema de gestión de seguridad de la información (SGSI). Se llevarán a cabo auditorías internas cada 12 meses y auditorías externas conforme a las exigencias regulatorias y contractuales.

6. Responsabilidades

- **Alta Dirección:** Asegurar la implementación de la política y asignación de recursos adecuados.
- **Departamento de Seguridad de la Información:** Monitorear, evaluar y mejorar las prácticas de seguridad.

- **Usuarios Finales:** Cumplir con los lineamientos establecidos y reportar cualquier incidente de seguridad.

7. Conclusión

Nuestra organización reafirma su compromiso con la seguridad de la información, estableciendo esta **Política de Seguridad en la Utilización de Medios Electrónicos** como un marco de referencia para la gestión de riesgos y cumplimiento normativo. La aplicación de esta política es obligatoria para todos los empleados y terceros que interactúen con nuestros sistemas de información.

Fecha de emisión: 24/02/2025