




SISTEMA  
DE GESTIÓN INTEGRADA  
EN-ISO 9001, EN-ISO 14001, EN-ISO 27001, ENS

POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACION

INSTALACIÓN Y MANTENIMIENTO DE:

- Sistemas automáticos de detección de incendios.
- Sistemas manuales de alarma de incendios.
- Sistemas de comunicación de alarma de incendios.
- Sistemas de abastecimiento de agua contra incendios.
- Sistemas de extintores de incendio.
- Sistemas de hidrantes contra incendios.
- Sistemas extintores de incendios.
- Sistemas de bocas de incendio equipadas.
- Sistemas de columna seca contra incendios.
- Sistema de extinción de rociadores automáticos.
- Sistemas de extinción de agua pulverizada.
- Sistemas de extinción de espuma física.
- Sistemas de extinción por polvo.
- Sistemas de extinción por agentes extintores gaseosos.
- Sistemas de extinción por aerosoles condensados.
- Sistemas para el control de humos y de calor.
- Sistemas de señalización luminiscente
- De aparatos, dispositivos y sistemas de seguridad
- Sistemas de video vigilancia.
- De control de accesos
- De dispositivos de Geolocalización (GPS) y plataforma de gestión de flotas

<b>Cambios respecto a la edición anterior:</b> Edición inicial		
<b>Elaborado por:</b> Óscar Alamillo Miquel Cusiné Calidad/MA/SGSI	<b>Aprobado por:</b> Alexandre Arqués Martí <b>Dirección.</b> 	<b>Edición: 0</b>
		<b>Fecha: 10/01/2024</b> <b>Revisado: 10/01/2024</b>





## Políticas Específicas de Seguridad de la Información (ISO 27001 y ENS)

Estas políticas específicas deben complementarse con las políticas generales de seguridad de la información de la empresa, basadas en ISO 27001 y ENS.

### 1. Política de Gestión de Acceso a Sistemas de Videovigilancia y Seguridad:

- **1.1. Propósito:**
  - Establecer los procedimientos para controlar el acceso a los sistemas de videovigilancia y seguridad, asegurando que solo el personal autorizado pueda acceder a la información y a los dispositivos.
  
- **1.2. Alcance:**
  - Esta política se aplica a todos los sistemas de videovigilancia y seguridad instalados y mantenidos por la empresa.
- **1.3. Controles:**
  - Implementación de autenticación multifactor (MFA) para el acceso a paneles de control y grabaciones.
  - Asignación de roles de acceso basados en el principio de mínimo privilegio.
  - Registro detallado de todos los accesos y modificaciones en los sistemas.
  - Revisión periódica de los permisos de acceso y eliminación de cuentas inactivas.
  - Cifrado de las comunicaciones entre los dispositivos y los sistemas de control.

### 2. Política de Gestión de Grabaciones de Videovigilancia:

- **2.1. Propósito:**
  - Establecer los procedimientos para la gestión segura de las grabaciones de videovigilancia, protegiendo la privacidad de los clientes y cumpliendo con la normativa aplicable (RGPD/LOPDGDD).



## POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACION

- **2.2. Alcance:**
  - Esta política se aplica a todas las grabaciones de videovigilancia generadas por los sistemas instalados y mantenidos por la empresa.
- **2.3. Controles:**
  - Cifrado de las grabaciones de video almacenadas en los servidores.
  - Implementación de políticas de retención y eliminación de grabaciones, basadas en los requisitos legales y contractuales.
  - Control de acceso estricto a las grabaciones, limitando el acceso al personal autorizado y a los clientes que lo soliciten.
  - Registro detallado de todos los accesos y copias de las grabaciones.
  - Procedimientos para la entrega segura de grabaciones a las autoridades competentes.

### 3. Política de Mantenimiento de Sistemas de Incendios:

- **3.1. Propósito:**
  - Establecer los procedimientos para el mantenimiento seguro de los sistemas de detección y extinción de incendios, garantizando su correcto funcionamiento y protegiendo la seguridad de las personas y los bienes.
- **3.2. Alcance:**
  - Esta política se aplica a todos los sistemas de incendios instalados y mantenidos por la empresa.
- **3.3. Controles:**
  - Realización de inspecciones y pruebas periódicas de los sistemas, siguiendo las recomendaciones del fabricante y la normativa aplicable.
  - Mantenimiento preventivo y correctivo de los dispositivos y equipos.
  - Registro detallado de todas las actividades de mantenimiento.
  - Formación del personal en el uso y mantenimiento de los sistemas.
  - Procedimientos para la notificación y gestión de fallos y alarmas.

### 4. Política de Gestión de Dispositivos Móviles de Técnicos:

- **4.1. Propósito:**
  - Establecer los procedimientos para el uso seguro de los dispositivos móviles utilizados por los técnicos, protegiendo la información de la empresa y de los clientes.
- **4.2. Alcance:**
  - Esta política se aplica a todos los dispositivos móviles (teléfonos, tabletas, portátiles, etc.) utilizados por los técnicos en el desempeño de sus funciones.



### • 4.3. Controles:

- Cifrado de los datos almacenados en los dispositivos.
- Implementación de software de gestión de dispositivos móviles para la gestión remota y el control de los dispositivos.
- Políticas de contraseñas fuertes y bloqueo automático de pantalla.
- Procedimientos para la notificación y gestión de pérdida o robo de dispositivos.
- Restricciones de instalación de aplicaciones no autorizadas.

## 5. Política de Endurecimiento de Sistemas Operativos y Aplicaciones

### 5.1. Propósito:

- Establecer los procedimientos para endurecer los sistemas operativos y aplicaciones utilizados por la empresa, reduciendo su superficie de ataque y protegiéndolos contra posibles vulnerabilidades.
- Cumplir con los requisitos de ISO 27001 y ENS en materia de seguridad de sistemas.
- Se debe de tener un especial cuidado en el cumplimiento de la normativa vigente en materia de protección de datos.
- Es de vital importancia una correcta gestión de los sistemas de protección contra incendios.

### 5.2. Alcance:

- Esta política se aplica a todos los sistemas operativos y aplicaciones utilizados por la empresa, incluyendo los instalados en servidores, estaciones de trabajo, dispositivos móviles y sistemas de videovigilancia, seguridad e incendios.

### 5.3. Responsabilidades:

- El equipo de seguridad de la información (técnico, administradores de sistemas, ingenieros de redes y analistas de seguridad) es responsable de la implementación y mantenimiento de los procedimientos de endurecimiento.

### 5.4. Procedimientos de Endurecimiento:

Se utiliza herramientas automatizadas para facilitar la implementación y el mantenimiento de los procedimientos de endurecimiento.



- **5.4.1. Sistemas Operativos:**
  - **5.4.1.1. Configuración Segura:**
    - Deshabilitar servicios y funcionalidades innecesarias.
    - Configurar contraseñas fuertes y políticas de bloqueo de cuentas.
    - Limitar los privilegios de los usuarios y grupos.
    - Habilitar el registro de eventos de seguridad (logs).
    - Configurar firewalls locales y reglas de acceso restrictivas.
  - **5.4.1.2. Actualizaciones y Parches:**
    - Implementar un proceso de gestión de parches para aplicar las actualizaciones de seguridad de forma oportuna.
    - Utilizar herramientas de gestión de parches automatizadas.
    - Realizar pruebas de compatibilidad antes de aplicar las actualizaciones en entornos de producción.
  - **5.4.1.3. Auditoría y Monitorización:**
    - Realizar auditorías de seguridad periódicas para verificar el cumplimiento de los procedimientos de endurecimiento.
    - Implementar herramientas de monitorización de logs y alertas de seguridad.
- **5.4.2. Aplicaciones:**
  - **5.4.2.1. Configuración Segura:**
    - Deshabilitar funcionalidades innecesarias y puertos de red no utilizados.
    - Configurar contraseñas fuertes y políticas de control de acceso.
    - Utilizar cifrado para proteger los datos sensibles almacenados y transmitidos por las aplicaciones.
    - Aplicar las recomendaciones de seguridad del fabricante de la aplicación.
  - **5.4.2.2. Actualizaciones y Parches:**
    - Mantener las aplicaciones actualizadas con los últimos parches de seguridad.
    - Utilizar repositorios de software confiables.
    - Realizar pruebas de seguridad antes de implementar nuevas versiones de las aplicaciones.
  - **5.4.2.3. Auditoría y Monitorización:**
    - Realizar pruebas de seguridad de las aplicaciones (análisis de vulnerabilidades, pruebas de penetración).
    - Monitorizar los logs de las aplicaciones para detectar actividades sospechosas.



- **5.4.3. Sistemas de Videovigilancia, Seguridad e Incendios:**
  - **5.4.3.1. Configuración Segura:**
    - Cambiar las contraseñas predeterminadas de los dispositivos y sistemas.
    - Deshabilitar funcionalidades innecesarias y puertos de red no utilizados.
    - Segmentar la red para aislar los sistemas de videovigilancia, seguridad e incendios.
    - Utilizar cifrado para proteger las comunicaciones entre los dispositivos y los sistemas de control.
  - **5.4.3.2. Actualizaciones y Parches:**
    - Mantener el firmware de los dispositivos actualizado con los últimos parches de seguridad.
    - Utilizar repositorios de firmware confiables.
    - Realizar pruebas de compatibilidad antes de actualizar el firmware en entornos de producción.
  - **5.4.3.3. Auditoría y Monitorización:**
    - Realizar auditorías de seguridad periódicas de los sistemas de videovigilancia, seguridad e incendios.
    - Monitorizar los logs de los dispositivos y sistemas para detectar actividades sospechosas.

### 5.5. Cumplimiento con ISO 27001 y ENS:

- Los procedimientos de endurecimiento se basan en los controles de seguridad establecidos en la norma ISO 27001 y el Esquema Nacional de Seguridad (ENS).
- Se documentan los procedimientos de endurecimiento y se mantienen registros de las actividades realizadas.
- Se realizan auditorías de seguridad periódicas para verificar el cumplimiento de los requisitos de ISO 27001 y ENS.

### 5.6. Revisión y Actualización:

- Esta política se revisará y actualizará periódicamente para garantizar su eficacia y adecuación a los cambios en el entorno de amenazas y la normativa.



## 6. Política Específica de Control de Acceso

### 6.1. Propósito:

- Establecer los principios y directrices para controlar el acceso a los sistemas de información, datos e instalaciones de la empresa, garantizando que solo el personal autorizado pueda acceder a los recursos necesarios para el desempeño de sus funciones.
- Cumplir con los requisitos de ISO 27001 y ENS en materia de control de acceso.

### 6.2. Alcance:

- Esta política se aplica a todos los sistemas de información, datos e instalaciones de la empresa, incluyendo los sistemas de videovigilancia, seguridad e incendios.
- Aplica a todos los empleados, contratistas y terceros que tengan acceso a los recursos de la empresa.

### 6.3. Responsabilidades:

- El responsable de seguridad de la información (SGSI) es responsable de la elaboración, implementación y mantenimiento de esta política.
- Los administradores de sistemas y los responsables de área son responsables de la implementación de los controles de acceso en sus respectivos ámbitos.
- Todos los usuarios son responsables de cumplir con esta política y de proteger sus credenciales de acceso.

### 6.4. Principios del Control de Acceso:

Se utiliza herramientas automatizadas para facilitar la gestión de los controles de acceso.

- **6.4.1. Necesidad de Conocimiento (Need-to-know):** El acceso a la información y a los sistemas se concederá únicamente cuando sea necesario para el desempeño de las funciones del usuario.
- **6.4.2. Mínimo Privilegio (Least Privilege):** A los usuarios se les concederán los privilegios mínimos necesarios para realizar sus tareas.
- **6.4.3. Separación de Funciones (Segregation of Duties):** Se separarán las funciones críticas para evitar conflictos de interés y reducir el riesgo de fraude.
- **6.4.4. Registro de Accesos (Access Logging):** Se registrarán todos los accesos a los sistemas y a la información sensible.



## POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACION

- **6.4.5. Revisión Periódica (Periodic Review):** Se revisarán periódicamente los permisos de acceso para garantizar que sigan siendo apropiados.

### 6.5. Reglas de Control de Acceso:

- **6.5.1. Autenticación:**
  - Se utilizará autenticación multifactor (MFA) para el acceso a sistemas críticos (servidores, bases de datos, paneles de control de sistemas de seguridad e incendios).
  - Se exigirán contraseñas robustas y se implementarán políticas de cambio periódico de contraseñas.
  - Se prohibirá compartir contraseñas entre usuarios.
- **6.5.2. Autorización:**
  - Se implementará control de acceso basado en roles (RBAC) para asignar permisos según las responsabilidades laborales.
  - Se utilizarán listas de control de acceso (ACLs) en firewalls y routers para controlar el tráfico de red.
  - Se revisarán y revocarán los accesos de los empleados que abandonan la empresa o cambian de puesto.
- **6.5.3. Control de Acceso Físico:**
  - Se controlará el acceso a las instalaciones mediante tarjetas de acceso, sistemas biométricos y videovigilancia.
  - Se protegerán los servidores y equipos críticos en salas seguras con acceso restringido.
  - Se implementarán medidas de seguridad para proteger los equipos de los clientes contra manipulaciones no autorizadas.
- **6.5.4. Gestión de Cuentas de Usuario:**
  - Se establecerán procedimientos para la creación, modificación y eliminación de cuentas de usuario.
  - Se utilizarán cuentas de usuario individuales para cada usuario.
  - Se deshabilitarán las cuentas de usuario inactivas.
- **6.5.5. Acceso Remoto:**
  - Se utilizarán conexiones VPN seguras para el acceso remoto a la red de la empresa.
  - Se implementarán controles de acceso adicionales para el acceso a los sistemas desde dispositivos móviles.
- **6.5.6. Acceso a Sistemas de Videovigilancia, Seguridad e Incendios:**
  - Se implementarán controles de acceso específicos para los sistemas de videovigilancia, seguridad e incendios, limitando el acceso al personal autorizado.
  - Se registrarán todos los accesos y modificaciones en los sistemas.



**6.6. Cumplimiento con ISO 27001 y ENS:**

- Los procedimientos de control de acceso se basan en los controles de seguridad establecidos en la norma ISO 27001 y el Esquema Nacional de Seguridad (ENS).
- Se documentan los procedimientos de control de acceso y se mantienen registros de las actividades realizadas.
- Se realizan auditorías de seguridad periódicas para verificar el cumplimiento de los requisitos de ISO 27001 y ENS.
- Se debe de tener un especial cuidado en el cumplimiento de la normativa vigente en materia de protección de datos.

**6.7. Revisión y Actualización:**

- Esta política se revisará y actualizará periódicamente para garantizar su eficacia y adecuación a los cambios en el entorno de amenazas y la normativa.
- Es de vital importancia una correcta gestión de los sistemas de protección contra incendios.

Se revisan y actualizan las políticas periódicamente para garantizar su eficacia.

Fdo.:



La Dirección