Manual de Seguridad de la Información - Sede de Barcelona

Tabla de contenidos

1 Introducción

Este manual tiene como propósito proporcionar un marco claro y consistente para proteger la información y los activos tecnológicos de la sede de Barcelona. Se trata de un documento vivo que establece las directrices fundamentales en materia de seguridad, en línea con las mejores prácticas y los requisitos normativos.

- **Propósito del manual:** Establecer políticas y procedimientos de obligado cumplimiento que aseguren la protección de la información tratada en esta sede, en especial la generada por los equipos de consultoría y soporte técnico para terceros.
- **Alcance:** Abarca todos los sistemas informáticos, plataformas cloud, aplicaciones internas, procesos de negocio y personal que accede a información corporativa desde o hacia la sede de Barcelona.
- **Público objetivo:** Aplica a empleados, proveedores, técnicos, subcontratistas, personal de mantenimiento con acceso a redes, y visitantes autorizados.

2 Principios de Seguridad de la Información

Los principios guían el diseño del Sistema de Gestión de Seguridad de la Información (SGSI):

- **Confidencialidad:** Fundamental en una empresa de servicios tecnológicos donde se trata información de clientes. Solo deben acceder los usuarios con necesidad legítima.
- **Integridad:** Se protege la fiabilidad de informes técnicos, configuraciones y registros de actividad.
- **Disponibilidad:** Los servicios de soporte deben estar operativos, por lo que se priorizan medidas de continuidad (copias de seguridad, redundancias).
- **Autenticidad:** Las conexiones y accesos deben estar verificados, especialmente al operar desde distintas ubicaciones.
- **Trazabilidad:** Cada acceso o acción relevante debe quedar registrada para fines forenses o de auditoría.

3 Marco Normativo y Regulatorio

- **ISO/IEC 27001:** La implantación de controles del Anexo A en TechSys Solutions guía este manual.
- **MAGERIT v3.0:** Utilizada para los análisis de riesgos presentados en el informe de Barcelona.
- **RGPD y LOPDGDD:** Por tratarse de datos personales de empleados y clientes.

4 Organización de la Seguridad

- **Responsable de seguridad en Barcelona:** Coordina acciones locales como gestión de incidentes, control de accesos y seguimiento de auditorías.
- **Usuarios:** Deben conocer las políticas de seguridad que aceptan mediante firma o validación digital.
- **Comité de Seguridad:** Revisión trimestral de indicadores y validación de planes correctivos.
- **Incidentes:** Se gestionan con trazabilidad completa una plataforma de tickets.

5 Clasificación y Manejo de la Información

La información manejada en TechSys Solutions se clasifica con base en su criticidad y el impacto potencial ante un acceso no autorizado. Esta clasificación guía el etiquetado, almacenamiento, transmisión y destrucción de la información.

- **Pública:** Información que puede ser difundida sin restricciones legales ni comerciales. Ejemplos: contenido de la página web corporativa, notas de prensa, portafolio de servicios públicos, políticas genéricas de calidad o medioambiente.
- **Interna:** Información de uso exclusivo dentro de la organización, cuyo acceso por terceros podría suponer un perjuicio menor. Ejemplos: instrucciones de trabajo internas, cronogramas de proyectos no sensibles, información de contacto entre empleados, manuales técnicos operativos no confidenciales.

- **Confidencial:** Información crítica cuyo acceso no autorizado puede tener un impacto severo en la organización o sus clientes. Ejemplos: documentación técnica de clientes, contratos comerciales, informes de incidentes de seguridad, análisis de riesgos, credenciales o configuraciones de sistemas, datos personales de empleados o usuarios.

El etiquetado de la información se aplica en formato físico (etiquetas visibles) y lógico (metadatos de archivos). El cifrado AES-256 se impone para la información confidencial tanto en tránsito como en reposo. La eliminación de información confidencial se lleva a cabo mediante borrado seguro (software certificado) o trituración mecánica de documentos impresos. Además, los empleados reciben formación sobre el manejo correcto de cada nivel de clasificación y sus implicaciones legales y operativas.

6 Control de Acceso

- **Autenticación:** MFA obligatorio en accesos remotos y sistemas cloud.
- **Autorización:** Se define por perfil (soporte, gestión, administración) y se revisa cada seis meses.
- **Gestión de cuentas:** Todo alta/baja se formaliza desde RRHH a TI mediante formularios aprobados.
- **Acceso remoto:** VPN corporativa + token OTP. Se controla el horario de conexión.

7 Seguridad Física y Ambiental

La sede está equipada con:

- **Control de accesos:** Puerta con lector de tarjetas, logs de entrada.
- **Equipos:** Rack cerrado bajo llave, estaciones protegidas contra acceso físico.
- **Ambiente:** Sensores de temperatura y humedad en sala técnica, extintores y sistema antiincendios.

8 Uso Aceptable de los Recursos Tecnológicos

- **Equipamiento:** Solo se permite el uso para fines laborales. Está prohibido el uso de dispositivos personales sin MDM.
- **Redes:** La Wi-Fi de invitados está segregada. No se permite el puenteo de red desde portátiles corporativos.
- **Correo y navegación:** Filtrado de spam, antivirus perimetral y bloqueo de sitios peligrosos.
- **Dispositivos externos:** Solo permitidos si están cifrados. Se registra su uso.

9 Gestión de Contraseñas

- **Requisitos:** 12 caracteres, al menos una mayúscula, número y carácter especial.
- **Rotación:** Cada 90 días, no se pueden reutilizar las 5 últimas contraseñas.
- **Gestores corporativos:** Se proporciona un gestor de contraseñas preconfigurado. Prohibido almacenar claves en navegadores.

10 Gestión de Copias de Seguridad

- **Frecuencia:** Diario en servidores y servicios cloud. Semanal en puestos críticos.
- **Procedimientos:** Basados en el plan de respaldo en HSM. Validado trimestralmente.
- **Pruebas:** Se realiza restauración simulada en entorno de pruebas dos veces al año.

11 Seguridad en Redes y Comunicaciones

- **Segmentación:** VLAN para administración, técnicos y consultores.
- **Cifrado:** Toda transmisión de datos se realiza por HTTPS, SFTP o VPN IPsec.
- **Monitoreo:** SIEM corporativo detecta eventos anómalos y lanza alertas automáticas.

12 Gestión de Incidentes de Seguridad

- **Incidentes:** Incluyen accesos indebidos, malware detectado, fuga de información.
- **Notificación:** Dentro de las primeras 4 horas al canal establecido.
- **Tratamiento:** Se aplica la política de respuesta rápida (contenida en otro documento anexo).
- **Registro:** Cada incidente se documenta para análisis y mejora.

13 Gestión de Actualizaciones y Parches

- **Planificación:** TI aplica parches cada segundo martes del mes.
- **Pruebas:** Antes en entorno sandbox. Las actualizaciones críticas se evalúan con prioridad.

14 Uso de Software

- **Control de versiones:** Centralizado. Se utiliza inventario automatizado.
- **Licencias:** Toda instalación debe contar con licencia válida. Se audita semestralmente.
- **Open source:** Debe pasar por revisión técnica y de licencias antes de su uso.

15 Formación y Concienciación

- **Formación inicial:** Cada empleado recibe formación al incorporarse.
- **Anual:** Módulo de ciberseguridad obligatorio.
- **Simulacros:** Phishing cada 4 meses. Se mide tasa de clics e informe a RRHH.

16 Revisión, Auditoría y Cumplimiento

- **Revisión:** El manual se revisa anualmente y tras auditorías o incidentes graves.
- **Auditorías:** Internas cada 6 meses. Externas anuales para renovación ISO.
- **Medidas disciplinarias:** Graduadas según política de sanciones internas.

17 Aprobación y Entrada en Vigor

- Documento aprobado por la Dirección General y por el responsable de seguridad.
- Entrada en vigor: 25/07/2025.
- Próxima revisión: 25/08/2026.