TechSys Solutions S.L.

Política de Seguridad de la Información

Versión: 1.0

Fecha de emisión: 15/5/2025

Responsable: Departamento de Seguridad de la Información

Aprobado por: Dirección General

Ubicación: Madrid – Barcelona – Sevilla – Teletrabajo

Índice

1. Propósito

El propósito de esta Política de Seguridad de la Información es establecer un marco general que permita proteger adecuadamente los activos de información de *TechSys Solutions S.L.*, garantizando su **confidencialidad, integridad y disponibilidad** frente a amenazas internas y externas.

Dado que la empresa desarrolla software y ofrece servicios de consultoría tecnológica, maneja datos sensibles tanto propios como de clientes. Por ello, esta política busca minimizar los riesgos asociados a la gestión de la información, los sistemas tecnológicos, y los dispositivos utilizados por el personal en sus distintas ubicaciones y modalidades de trabajo, incluyendo el teletrabajo.

Este documento sienta las bases para aplicar medidas de seguridad consistentes y alineadas con las mejores prácticas del sector, cumpliendo además con las normativas legales vigentes, especialmente en lo relativo a la protección de datos personales. También pretende fomentar una cultura de seguridad entre todos los empleados y colaboradores de la organización.

2. Alcance

Esta Política de Seguridad de la Información aplica a **todas las personas, procesos, tecnologías y ubicaciones** de *TechSys Solutions S.L.*, incluyendo:

- Las **tres sedes físicas** de la empresa: Madrid (sede central), Barcelona y Sevilla.
- Los **empleados en modalidad de teletrabajo**, sin importar su rol o ubicación geográfica.
- Todo el **personal interno**, así como colaboradores externos, proveedores de servicios tecnológicos y cualquier tercero que acceda o gestione información de la empresa.

El alcance comprende:

- **Toda la información** manejada por la empresa, en cualquier formato (digital o físico), ya sea propia o de clientes.
- Los **sistemas informáticos y redes** utilizados en la organización, incluyendo servidores, equipos de usuario, dispositivos móviles, aplicaciones y servicios en la

nube.

- Las **infraestructuras de seguridad**, como firewalls, VPNs, controles de acceso, y mecanismos de autenticación.

- Las **actividades diarias** relacionadas con la creación, acceso, procesamiento, almacenamiento, transmisión o eliminación de información.

Quedan fuera del alcance de esta política:

- Activos físicos o infraestructuras **no gestionados directamente por la empresa**, como espacios de coworking temporales sin control propio.

- **Equipos personales** utilizados en teletrabajo que no cumplan con los requisitos mínimos de seguridad definidos por la empresa.

3. Definiciones clave

- **Activo de información**: Todo recurso con valor para la organización relacionado con la información, incluyendo documentos, bases de datos, software, hardware, redes, servicios en la nube y conocimiento del personal.
- **Confidencialidad**: Propiedad de la información que garantiza que solo las personas autorizadas puedan acceder a ella.
- **Integridad**: Propiedad de la información que asegura que no ha sido alterada o manipulada de forma no autorizada.
- **Disponibilidad**: Capacidad de acceso a la información y a los sistemas cuando los usuarios autorizados lo necesitan.
- **Amenaza**: Potencial causa de un incidente que puede dañar un activo o causar pérdida de datos, reputación o recursos.
- **Vulnerabilidad**: Debilidad que puede ser explotada por una amenaza para causar daño a un activo o a la empresa.
- **Incidente de seguridad**: Evento que compromete o podría comprometer la confidencialidad, integridad o disponibilidad de la información o de los sistemas.
- **Usuario**: Persona con acceso autorizado a los sistemas o información de la empresa, incluyendo empleados, proveedores y colaboradores externos.
- **Administrador de sistemas**: Persona responsable de la gestión técnica y operativa de servidores, redes y sistemas de información.
- **Autenticación multifactor (MFA)**: Método de verificación que requiere al menos dos pruebas distintas de identidad (por ejemplo, contraseña y código temporal).
- **BYOD (Bring Your Own Device)**: Práctica que permite el uso de dispositivos personales para tareas laborales, bajo normas de seguridad definidas por la empresa.

- **Datos personales**: Cualquier información que pueda identificar directa o indirectamente a una persona física (nombre, DNI, email, dirección IP, etc.).
- **Datos sensibles**: Información personal especialmente protegida, como salud, religión, ideología, orientación sexual o datos financieros.
- **Phishing**: Técnica de ingeniería social que intenta engañar a los usuarios para obtener información confidencial, como credenciales o datos bancarios.
- **Firewall**: Sistema de seguridad que regula el tráfico de red permitiendo o bloqueando conexiones según reglas predefinidas.
- **VPN (Virtual Private Network)**: Red privada virtual que permite establecer conexiones cifradas y seguras entre dispositivos remotos y la red interna corporativa.
- **SIEM (Security Information and Event Management)**: Plataforma que centraliza, analiza y correlaciona eventos de seguridad provenientes de múltiples fuentes para detectar amenazas.
- **SGSI (Sistema de Gestión de Seguridad de la Información)**: Conjunto estructurado de políticas, procesos y herramientas para proteger los activos de información y gestionar los riesgos de seguridad.
- **Clasificación de la información**: Proceso por el cual se categoriza la información según su nivel de sensibilidad y criticidad (por ejemplo: pública, interna, confidencial).
- **Acceso basado en roles (RBAC)**: Modelo de control de acceso que otorga permisos a los usuarios en función de su rol dentro de la organización.
- **Comité de Seguridad**: Órgano interno multidisciplinario que supervisa la implementación, evolución y cumplimiento de la política de seguridad y el SGSI.
- **Responsable de Seguridad de la Información (RSI)**: Persona designada para liderar y coordinar la seguridad de la información en la organización.
- **RTO (Recovery Time Objective)**: Tiempo máximo tolerable para la recuperación de un sistema o servicio tras una interrupción.
- **RPO (Recovery Point Objective)**: Punto máximo en el tiempo (medido desde la última copia de seguridad válida) desde el cual se pueden recuperar los datos sin pérdidas críticas.
- **Plan de Continuidad del Negocio (BCP)**: Estrategia organizativa para mantener la operatividad de procesos críticos durante y después de una interrupción grave.
- **Plan de Recuperación ante Desastres (DRP)**: Conjunto de procedimientos técnicos destinados a restaurar los sistemas de TI y servicios afectados por un evento disruptivo.
- **Simulacro**: Ejercicio planificado que pone a prueba la capacidad de respuesta de la organización ante incidentes, ya sea de forma práctica (mock drill) o teórica (tabletop).
- **No conformidad**: Situación en la que se detecta un incumplimiento con una política, norma interna, procedimiento o requisito establecido.

4. Comité de Seguridad

El Comité de Seguridad de la Información de *TechSys Solutions S.L.* es el órgano responsable de supervisar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Su misión principal es coordinar las acciones necesarias para garantizar la protección de los activos de información y el cumplimiento de esta política en toda la organización.

Composición del Comité

El comité estará integrado por los siguientes miembros:

- **Responsable de Seguridad de la Información (RSI)** – Preside el comité y coordina las actividades.
- **Responsable del Departamento de TI**
- **Representante de la Alta Dirección**
- **Representante del Área de Desarrollo de Software**
- **Representante de Consultoría/Atención al Cliente**
- **Representante de Finanzas y Comercial**
- **Representante de Recursos Humanos**
- **Delegado de Protección de Datos (cuando aplique)**

Adicionalmente, podrán ser convocados asesores externos o personal técnico específico cuando se traten temas particulares (auditorías, brechas, legal, etc.).

Funciones del Comité

- Establecer y revisar las políticas, procedimientos y controles de seguridad.
- Evaluar los riesgos de seguridad y definir acciones correctivas.
- Aprobar los planes de concienciación, formación y respuesta ante incidentes.
- Coordinar la respuesta ante incidentes graves de seguridad.
- Supervisar auditorías y revisiones internas del SGSI.

- Velar por el cumplimiento normativo (RGPD, LOPDGDD, etc.).

- Informar periódicamente a la Alta Dirección sobre el estado de la seguridad.

Reuniones

El comité se reunirá de forma **trimestral** y de manera extraordinaria siempre que ocurra un incidente crítico o haya que tomar decisiones urgentes relacionadas con la seguridad de la información.

5. Responsabilidades del personal

Todos los empleados, colaboradores y terceros con acceso a los sistemas o la información de *TechSys Solutions S.L.* tienen la responsabilidad de proteger los activos de información de la empresa. Esta responsabilidad incluye cumplir con las políticas, normas y procedimientos establecidos en este documento, así como actuar de forma proactiva ante situaciones que puedan representar un riesgo para la seguridad.

Responsabilidades generales para todo el personal:

- Conocer y cumplir esta Política de Seguridad de la Información.

- Utilizar los sistemas y dispositivos únicamente para fines autorizados y conforme a las políticas internas.

- Proteger las credenciales de acceso (usuario y contraseña) y no compartirlas con terceros.

- Notificar inmediatamente cualquier incidente, anomalía o sospecha de brecha de seguridad al área de TI o al Responsable de Seguridad.

- Mantener actualizados los dispositivos utilizados (tanto corporativos como personales en modalidad BYOD) con antivirus, parches y configuraciones exigidas.

- Asegurar la protección física de dispositivos portátiles y documentos con información sensible.

- Evitar la instalación de software no autorizado o proveniente de fuentes no verificadas.

- No almacenar información confidencial en medios no cifrados o sin respaldo.

Responsabilidades específicas según entorno:

Personal en oficinas (sedes físicas):

- Seguir las medidas de control de acceso físico y lógico establecidas.
- Bloquear su sesión cuando se aleje del puesto de trabajo.
- Destruir físicamente (o mediante trituradora) la documentación impresa con datos sensibles.

Teletrabajadores:

- Conectarse exclusivamente a través de la VPN corporativa y utilizando autenticación multifactor (MFA).
- Garantizar que su entorno de trabajo en casa sea seguro, libre de accesos no autorizados por parte de terceros o convivientes.
- Utilizar únicamente dispositivos que cumplan con las condiciones de seguridad definidas por la empresa (antivirus, cifrado de disco, etc.).

Colaboradores externos o proveedores:

- Cumplir con los acuerdos de confidencialidad firmados.
- Respetar las políticas de seguridad aplicables durante el tiempo que tengan acceso a los sistemas o información de TechSys Solutions S.L.

6. Responsabilidades del departamento de TI

El Departamento de Tecnologías de la Información (TI) de *TechSys Solutions S.L.* es responsable de planificar, implementar, administrar y supervisar las medidas técnicas necesarias para garantizar la seguridad de la información y la continuidad de los sistemas y servicios.

Funciones principales:

- **Gestión de accesos**: Crear, modificar y revocar cuentas de usuario de acuerdo con las autorizaciones asignadas a cada rol. Aplicar principios de mínimo privilegio y necesidad de conocimiento.
- **Administración de infraestructuras**:

    - Mantener actualizados servidores, redes, sistemas operativos y dispositivos corporativos.

    - Configurar firewalls, VPNs, IDS/IPS y otros mecanismos de protección.

    - Supervisar las conexiones remotas (VPN, teletrabajo) y aplicar controles de seguridad específicos.

- **Copia de seguridad y recuperación**:

    - Gestionar copias de seguridad regulares de la información crítica, tanto en las sedes físicas como en entornos cloud.

    - Comprobar periódicamente la integridad de los backups y realizar pruebas de restauración.

- **Gestión de incidentes**:

    - Actuar como primera línea de respuesta ante incidentes técnicos o de ciberseguridad.

    - Documentar y escalar los incidentes según el procedimiento establecido.

    - Colaborar en el análisis forense y recuperación posterior.

- **Actualización y parches**:

    - Garantizar la instalación oportuna de actualizaciones de seguridad en todos los sistemas y aplicaciones.

- **Soporte técnico seguro**:

    - Brindar asistencia a usuarios sin comprometer la seguridad, verificando identidades y registrando actividades de soporte.

- **Gestión de dispositivos**:

    - Controlar el inventario de equipos y su configuración.

    - Aplicar políticas de cifrado de disco, antivirus, y control de dispositivos extraíbles.

- **Supervisión y monitoreo**:

    - Implementar sistemas de registro y auditoría (logs).

    - Monitorear el tráfico de red, los accesos y las alertas de seguridad.

Coordinación con otros departamentos

El área de TI deberá trabajar en conjunto con Recursos Humanos, Legal y el Comité de Seguridad para asegurar que las medidas técnicas se alineen con las políticas internas, la normativa vigente y las necesidades reales de la organización.

7. Identificación de riesgos

La identificación de riesgos es una actividad fundamental para proteger los activos de información de *TechSys Solutions S.L.* Consiste en reconocer los elementos que pueden afectar la confidencialidad, integridad o disponibilidad de los datos, sistemas y servicios críticos de la organización.

Objetivo

Detectar de forma proactiva los posibles eventos, debilidades o situaciones que puedan derivar en incidentes de seguridad, para luego evaluarlos y tratarlos adecuadamente.

Áreas consideradas en la identificación de riesgos

1. **Infraestructura tecnológica**
    - Fallos de hardware o software en servidores, estaciones de trabajo y redes.
    - Configuraciones incorrectas o inseguras en dispositivos de red y firewalls.
    - Acceso remoto sin protección suficiente.
2. **Sistemas de información y aplicaciones**
    - Código vulnerable en aplicaciones propias.
    - Fugas de información por interfaces API mal aseguradas.
    - Dependencia de servicios en la nube y terceros.
3. **Usuarios y errores humanos**
    - Uso de contraseñas débiles o compartidas.
    - Descuidos en el manejo de datos sensibles.
    - Falta de formación en seguridad y respuesta ante amenazas como phishing.

4. **Dispositivos y movilidad**
    - Robo o pérdida de portátiles y smartphones.
    - Equipos personales (BYOD) sin las medidas mínimas de seguridad.
    - Accesos a la red desde redes Wi-Fi públicas o inseguras.
5. **Factores externos**
    - Ataques dirigidos (ransomware, denegación de servicio, etc.).
    - Proveedores que no cumplen con los estándares de seguridad.
    - Fallos en el suministro eléctrico o conectividad.
6. **Cumplimiento normativo**
    - Posibles incumplimientos del RGPD u otras normativas de protección de datos.
    - Ausencia de registros o trazabilidad de ciertos procesos críticos.

Fuentes de identificación

- Inventario de activos de información.
- Revisión de incidentes anteriores.
- Evaluaciones internas y auditorías.
- Reuniones del Comité de Seguridad.
- Herramientas automáticas de detección y monitoreo.

8. Evaluación y análisis de riesgos

Una vez identificados los posibles riesgos, *TechSys Solutions S.L.* realiza su evaluación con el fin de determinar la probabilidad de ocurrencia y el impacto potencial sobre los activos de información. Esto permite priorizar adecuadamente los esfuerzos y recursos destinados a la seguridad.

Objetivo

Establecer un enfoque sistemático para medir el nivel de riesgo asociado a cada amenaza, considerando tanto aspectos técnicos como humanos y organizativos.

Metodología

La evaluación se basa en dos dimensiones:

- **Probabilidad**: Estimación de la frecuencia con la que podría ocurrir un incidente asociado al riesgo.
- **Impacto**: Nivel de daño que produciría dicho incidente sobre la organización, sus operaciones, reputación o cumplimiento legal.

Ambos valores se clasifican, por ejemplo, como:

- **Bajo**, **Medio** o **Alto**

Y se combinan para obtener un **nivel de riesgo**:

- **Crítico**, **Alto**, **Moderado**, **Aceptable**

Esta clasificación se realiza mediante una **matriz de riesgos** que ayuda a visualizar la prioridad de tratamiento para cada caso.

Criterios de análisis

Se tendrán en cuenta los siguientes elementos:

- Tipo de activo afectado (datos personales, financieros, código fuente, etc.)
- Rol o departamento expuesto al riesgo.
- Controles existentes y su nivel de eficacia.

- Dependencia de sistemas o terceros para la continuidad del negocio.
- Requisitos legales y contractuales aplicables (RGPD, acuerdos con clientes, etc.)

Resultado del análisis

El resultado es un **informe de riesgos priorizados**, que alimenta el Plan de Tratamiento de Riesgos (ver punto siguiente), y se revisa de forma periódica por el Comité de Seguridad.

9. Plan de tratamiento de riesgos

El Plan de Tratamiento de Riesgos define las acciones que *TechSys Solutions S.L.* implementará para mitigar, reducir o controlar los riesgos identificados durante el proceso de análisis. Su objetivo es proteger la información y los sistemas críticos, garantizando la continuidad del negocio y el cumplimiento normativo.

Objetivos del tratamiento

- Reducir los riesgos a niveles aceptables según los criterios de la empresa.
- Priorizar medidas según el impacto y la probabilidad del riesgo.
- Asignar responsables claros para cada acción.

Estrategias de tratamiento posibles

Para cada riesgo evaluado, se determinará una de las siguientes estrategias:

- **Mitigar**: Implementar medidas técnicas u organizativas que reduzcan la probabilidad o el impacto del riesgo (por ejemplo, cifrado de datos, copias de seguridad, segmentación de red).
- **Evitar**: Eliminar el origen del riesgo, por ejemplo, descontinuando un sistema inseguro o un servicio no indispensable.
- **Transferir**: Delegar el riesgo parcial o totalmente a un tercero, mediante seguros o acuerdos con proveedores.

- **Aceptar**: Decidir conscientemente asumir el riesgo sin aplicar acciones adicionales, cuando se considera de bajo impacto o costo inasumible su mitigación.

Ejemplos de acciones concretas

- Implementar autenticación multifactor (MFA) para accesos remotos.
- Actualizar sistemas operativos obsoletos en sedes regionales.
- Cifrar discos duros de portátiles y smartphones corporativos.
- Definir políticas BYOD más estrictas para teletrabajadores.
- Formalizar acuerdos de confidencialidad con proveedores externos.

Asignación y seguimiento

- Cada acción será asignada a un responsable técnico o administrativo.
- Se establecerá un plazo de ejecución y una fecha de revisión.
- El Comité de Seguridad realizará un seguimiento periódico del avance y eficacia de las medidas adoptadas.

10. Control de acceso

El control de acceso es fundamental para proteger los activos de información de *TechSys Solutions S.L.*. Este control garantiza que solo las personas autorizadas puedan acceder a los sistemas, aplicaciones, redes y datos, de acuerdo con sus funciones y responsabilidades.

Principios generales

- **Acceso basado en roles (RBAC)**: Cada usuario accede solo a la información y recursos necesarios para su trabajo.
- **Mínimo privilegio**: Se otorgan los permisos mínimos indispensables para realizar las tareas asignadas.

- **Necesidad de conocimiento**: La información sensible sólo debe ser accesible por quienes realmente la necesitan.

Tipos de acceso

- **Acceso lógico**: Controlado mediante credenciales (usuario/contraseña) y autenticación multifactor (MFA) en sistemas internos, VPN y aplicaciones en la nube.
- **Acceso físico**: Controlado mediante tarjetas identificativas, controles biométricos y registros en las sedes corporativas.

Medidas técnicas

- Autenticación multifactor obligatoria para accesos remotos y servicios críticos.
- Contraseñas robustas con renovación periódica.
- Bloqueo automático de sesiones inactivas.
- Restricción de acceso a redes mediante listas blancas de dispositivos autorizados.
- Segmentación de red por departamentos (VLANs en sede central).
- Control de accesos administrativos con registro de actividad (logs).

Procedimientos

- Altas, modificaciones y bajas de usuarios gestionadas por el departamento de TI bajo solicitud autorizada.
- Revisión periódica de permisos y cuentas activas, especialmente en cambios de puesto o bajas de personal.
- Auditorías internas para verificar el cumplimiento de las políticas de acceso.

Accesos especiales

- Los accesos privilegiados (administradores, desarrolladores con acceso a producción, etc.) deben estar debidamente justificados, controlados y monitorizados.

11. Seguridad de contraseñas

Las contraseñas son una de las primeras líneas de defensa para proteger los sistemas y la información de *TechSys Solutions S.L.*. Una mala gestión de las mismas puede poner en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Requisitos de contraseñas

Todas las contraseñas utilizadas para acceder a sistemas corporativos deben cumplir con los siguientes criterios mínimos:

- Longitud mínima de **12 caracteres**.
- Incluir al menos **una letra mayúscula, una minúscula, un número y un carácter especial**.
- No contener palabras evidentes como nombres personales, de la empresa o secuencias simples ("1234", "abcd", etc.).
- No repetir contraseñas anteriores.
- No compartirse bajo ningún concepto con otros usuarios.

Buenas prácticas obligatorias

- Se recomienda el uso de un **gestor de contraseñas** autorizado por el departamento de TI para generar y almacenar claves seguras.
- **Cambiar inmediatamente** la contraseña si se sospecha de compromiso o si ha sido compartida accidentalmente.
- No almacenar contraseñas en notas, archivos sin cifrado ni navegadores sin protección.
- Utilizar **contraseñas únicas** para cada sistema o aplicación (no reutilizarlas).

Autenticación multifactor (MFA)

El uso de autenticación multifactor es obligatorio para los siguientes casos:

- Acceso remoto (VPN, correo, escritorio virtual, etc.).
- Servicios en la nube que contengan información confidencial o datos personales.

- Cuentas de administración o con privilegios elevados.

Gestión y caducidad

- Las contraseñas deben renovarse **cada 90 días** en cuentas críticas (por ejemplo, acceso a servidores, bases de datos o aplicaciones con información sensible).

- El departamento de TI debe mantener un sistema de control para forzar el cambio cuando corresponda y para gestionar las solicitudes de recuperación de acceso de forma segura.

12. Gestión de activos de información

La correcta gestión de los activos de información permite a *TechSys Solutions S.L.* conocer, clasificar y proteger adecuadamente todos los elementos que tienen valor para la organización, tanto físicos como digitales.

Identificación y registro de activos

- Todos los activos relacionados con la información (hardware, software, bases de datos, documentos, cuentas, etc.) deben ser **inventariados** y registrados por el departamento de TI.

- El inventario debe mantenerse **actualizado** y contar con información mínima como:

    - Tipo de activo

    - Responsable

    - Ubicación

    - Clasificación de la información asociada

    - Estado (activo, en reparación, fuera de uso)

Clasificación de activos

Los activos deben clasificarse según el nivel de sensibilidad de la información que contienen o procesan. Por ejemplo:

- **Confidencial**: Información crítica para la empresa, datos de clientes, contratos, código fuente.

- **Interno**: Información de uso restringido dentro de la empresa.

- **Público**: Información sin restricciones de difusión.

Esta clasificación se reflejará en las políticas de uso, control de acceso, y protección de cada activo.

Asignación de responsabilidades

- Cada activo debe tener un **responsable designado**, encargado de su uso adecuado, protección, actualización y eliminación segura cuando corresponda.

- Los usuarios deben firmar un **documento de aceptación** al recibir un dispositivo, en el que se detallen las condiciones de uso.

Uso y mantenimiento

- Todos los dispositivos deben tener **antivirus actualizado**, **cifrado de disco** (cuando aplique), y cumplir con las configuraciones de seguridad definidas.

- No se permite la instalación de software no autorizado.

- Los sistemas deben mantenerse **actualizados con los últimos parches** de seguridad.

Eliminación y baja de activos

- Al finalizar la vida útil de un activo, este debe ser **formateado, borrado de forma segura o destruido físicamente** según el tipo de información que haya contenido.

- Se deben seguir procedimientos específicos de **borrado seguro de datos** para evitar recuperaciones indebidas.

13. Uso aceptable de sistemas y dispositivos

Esta sección define las normas de uso aceptable de los sistemas informáticos, redes y dispositivos de *TechSys Solutions S.L.*, tanto en sedes físicas como en modalidad de teletrabajo. El objetivo es asegurar que estos recursos se utilicen de forma segura, ética y conforme a los fines de la empresa.

Dispositivos autorizados

- Solo se permite el uso de **dispositivos corporativos** o **dispositivos personales que cumplan con los requisitos BYOD** establecidos por la empresa (antivirus, cifrado, sistema operativo actualizado).

- Está prohibido conectar equipos o unidades externas (USB, discos duros, etc.) sin autorización expresa del departamento de TI.

Uso responsable

- Los dispositivos y cuentas de usuario deben usarse exclusivamente para **fines laborales**.

- No se permite el acceso a contenidos ilegales, inapropiados o no relacionados con la actividad de la empresa.

- No se deben instalar aplicaciones no autorizadas ni realizar modificaciones sobre configuraciones de seguridad.

Buenas prácticas obligatorias

- **Bloquear la pantalla** al ausentarse del puesto de trabajo.

- Mantener actualizado el sistema operativo, el antivirus y el software instalado.

- No almacenar credenciales o información sensible en texto plano.

- Evitar el uso de redes Wi-Fi públicas sin protección (usar VPN siempre que se trabaje fuera de la oficina).

Uso del correo electrónico corporativo

- Utilizarlo exclusivamente para comunicaciones laborales.

- No reenviar información confidencial sin autorización.

- Extremar precauciones ante correos sospechosos (phishing, archivos adjuntos extraños, etc.).

Acceso remoto y teletrabajo

- El acceso remoto a los sistemas de la empresa debe realizarse exclusivamente mediante **VPN corporativa** y con **autenticación multifactor (MFA)**.
- El equipo utilizado debe estar protegido con **contraseña, cifrado de disco y antivirus activo**.
- Se recomienda trabajar desde un espacio privado y seguro, evitando el acceso visual o auditivo de terceros.

Prohibiciones específicas

- Compartir contraseñas o cuentas de usuario.
- Utilizar los recursos de la empresa para actividades personales que comprometan la seguridad.
- Desactivar funciones de seguridad (firewalls, antivirus, bloqueos automáticos).

Consecuencias del uso indebido

El uso inadecuado de los recursos tecnológicos puede derivar en **sanciones disciplinarias**, **pérdida de acceso**, o incluso **acciones legales**, dependiendo de la gravedad de la infracción.

14. Seguridad en la red

La seguridad de las redes de comunicación es fundamental para proteger los datos, los sistemas y la operación continua de *TechSys Solutions S.L.*. Esto aplica tanto a las redes internas de las sedes físicas como a las conexiones remotas desde dispositivos móviles y entornos de teletrabajo.

Principios generales

- Todas las redes deben estar **segmentadas**, protegidas y monitorizadas.
- Se debe garantizar la **confidencialidad, integridad y disponibilidad** de la información que circula a través de ellas.

Controles implementados

1. Red corporativa (sede central y sedes regionales):

- Segmentación por VLAN según área o departamento (TI, Desarrollo, Finanzas, etc.).
- Firewall de nueva generación (NGFW) en la sede central para filtrar tráfico y detectar amenazas.
- Firewalls locales en sedes regionales con políticas adaptadas según funciones.
- Red Wi-Fi protegida con cifrado WPA2/WPA3 y autenticación 802.1X.
- Acceso a red restringido a dispositivos autorizados.

2. Acceso remoto (teletrabajadores):

- Acceso exclusivo mediante **VPN corporativa** con MFA.
- Verificación de dispositivo, antivirus y cumplimiento de políticas BYOD antes de conexión.
- Limitación de acceso remoto según rol o perfil de usuario.

3. Seguridad perimetral y tráfico saliente:

- Políticas de salida estrictas desde la red interna hacia internet.
- Inspección de tráfico HTTPS y aplicaciones en la nube.
- Detección de comportamientos anómalos mediante sistemas IDS/IPS y registros centralizados (SIEM).

4. Supervisión y registros:

- Monitorización continua del tráfico interno y externo.

- Registros de conexiones VPN, accesos a servidores y cambios de configuración.
- Alertas automáticas ante patrones de ataque, conexiones sospechosas o exfiltración de datos.

Medidas adicionales

- Revisión periódica de reglas de firewall y configuración de red.
- Pruebas de penetración para detectar vulnerabilidades en los puntos de entrada.
- Uso de DNS con filtrado de malware y contenidos maliciosos.

15. Clasificación de la información

La clasificación de la información permite aplicar controles de seguridad adecuados según la sensibilidad y el valor de los datos para *TechSys Solutions S.L.*. Esta práctica facilita la protección, el acceso controlado y el tratamiento correcto de la información en toda la organización.

Objetivos

- Establecer niveles claros de protección.
- Identificar la información crítica o sensible.
- Facilitar el cumplimiento de normativas como el RGPD.

Categorías de clasificación

Toda información generada, procesada o almacenada en la empresa deberá clasificarse en una de las siguientes categorías:

1. **Información Confidencial**

- Datos cuyo acceso no autorizado puede causar **daños graves** a la empresa o a terceros.

- Ejemplos: código fuente, bases de datos de clientes, credenciales de API, contratos confidenciales, estrategias corporativas.

- Acceso: restringido a personal autorizado. Cifrado obligatorio en almacenamiento y transmisión.

2. **Información Sensible**

    - Datos importantes cuyo acceso no autorizado podría generar impactos **moderados**.

    - Ejemplos: nóminas, facturación, estadísticas de ventas, datos de clientes potenciales.

    - Acceso: limitado por perfil. Requiere control de acceso y cifrado preferente.

3. **Información Interna**

    - Información de uso común dentro de la empresa, no crítica pero no pública.

    - Ejemplos: manuales internos, calendarios de actividades, informes de proyectos no confidenciales.

    - Acceso: personal interno autorizado. No requiere cifrado, pero sí medidas básicas de protección.

4. **Información Pública**

    - Información destinada a difusión externa sin riesgo para la organización.

    - Ejemplos: contenido web institucional, publicaciones en redes sociales, notas de prensa.

    - Acceso: sin restricciones.

Obligaciones del personal

- Toda persona que genere o maneje información debe **clasificarla correctamente** y aplicar las medidas de protección correspondientes.

- Los documentos deben ser **etiquetados o marcados**, siempre que sea posible, según su nivel de sensibilidad.

Revisión y actualización

La clasificación deberá ser revisada regularmente por los responsables de cada área, especialmente cuando se detecten cambios en la sensibilidad o exposición de los datos.

16. Retención y eliminación de datos

La gestión adecuada del ciclo de vida de la información permite a *TechSys Solutions S.L.* cumplir con las obligaciones legales, reducir riesgos de seguridad y optimizar el uso de recursos. Esto incluye definir cuánto tiempo debe conservarse la información y cómo eliminarla de forma segura cuando ya no sea necesaria.

Principios generales

- Los datos deben conservarse **únicamente durante el tiempo necesario** para cumplir con su finalidad específica o con lo establecido por la legislación vigente.
- Una vez cumplido ese período, deben ser **eliminados de forma segura y definitiva**.

Plazos de retención

Tipo de información	Tiempo mínimo de conservación	Base legal o criterio
Contratos y documentos legales	5 años	Código Civil / Comercial
Datos personales de empleados	Hasta 6 años tras baja laboral	RGPD / Ley laboral española
Información fiscal y contable	6 años	Normativa tributaria

Registros de actividad TI (logs)	Entre 6 meses y 2 años	Seguridad / Auditorías
Datos de clientes	Mientras exista relación + 5 años	RGPD / LOPDGDD
Currículums no seleccionados	1 año	Buenas prácticas y consentimiento
Backups de datos críticos	Según política de copias	Plan de continuidad

Nota: los plazos pueden variar en función de actualizaciones legales o nuevos contratos. La empresa debe revisarlos periódicamente.

Eliminación segura de datos

Cuando la información ya no es necesaria, deberá ser eliminada mediante métodos seguros, acordes al medio en que se encuentre:

- **Entorno digital**:
    - Borrado con software de sobrescritura segura.
    - Destrucción de unidades de almacenamiento si es necesario.
- **Formato físico**:
    - Destrucción mediante trituradora o servicios certificados de destrucción documental.

No se permite desechar documentos o soportes que contengan información sensible sin aplicar procedimientos de destrucción segura.

Responsabilidad

- Cada departamento es responsable de **controlar los plazos de retención** de su documentación.

- El departamento de TI supervisará la **eliminación segura de activos digitales**.
- El Comité de Seguridad coordinará revisiones periódicas del cumplimiento de esta política.

17. Privacidad y protección de datos personales

TechSys Solutions S.L. se compromete a cumplir con el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), y demás normativa aplicable en materia de privacidad. Este compromiso abarca tanto la protección de los datos personales como los derechos de las personas sobre su información.

Principios de tratamiento

Toda recopilación, tratamiento, almacenamiento o eliminación de datos personales debe cumplir con los siguientes principios:

- **Licitud, lealtad y transparencia**: Informar claramente a las personas sobre el uso de sus datos.
- **Limitación de la finalidad**: Usar los datos solo para los fines específicos para los que fueron recogidos.
- **Minimización de datos**: Recoger solo los datos necesarios.
- **Exactitud**: Mantener los datos actualizados.
- **Limitación del plazo de conservación**: No conservar datos personales más tiempo del necesario.
- **Integridad y confidencialidad**: Proteger los datos mediante medidas de seguridad adecuadas.

Derechos de los titulares de datos

La empresa garantizará a empleados, clientes y terceros el ejercicio de sus derechos:

- Acceso
- Rectificación
- Supresión ("derecho al olvido")
- Oposición
- Limitación del tratamiento
- Portabilidad de los datos

Las solicitudes serán gestionadas en coordinación con el **Delegado de Protección de Datos (DPO)**, si lo hubiere, o con el Responsable de Seguridad.

Medidas de protección aplicadas

- Cifrado de datos sensibles en reposo y en tránsito.
- Control de accesos basado en roles y necesidad de conocimiento.
- Registro de actividades de tratamiento.
- Contratos con encargados del tratamiento que incluyan cláusulas de confidencialidad y cumplimiento del RGPD.
- Evaluaciones de impacto en protección de datos (EIPD), cuando sea necesario.

Formación y concienciación

Todo el personal recibirá **formación básica en protección de datos personales**, especialmente quienes trabajen con datos sensibles (Atención al Cliente, Finanzas, Consultoría, RRHH).

18. Procedimiento de notificación de incidentes

TechSys Solutions S.L. establece un procedimiento formal para que cualquier persona de la organización pueda reportar incidentes de seguridad de la información de forma inmediata, clara y segura.

¿Qué se considera un incidente?

Un incidente de seguridad puede incluir, entre otros:

- Acceso no autorizado a datos, sistemas o cuentas.
- Pérdida o robo de dispositivos con información corporativa.
- Infecciones por malware, ransomware o virus.
- Fallos de seguridad en aplicaciones o servicios internos.
- Filtración de datos personales o confidenciales.
- Envío o recepción de correos sospechosos (phishing).
- Violación de políticas de seguridad por parte de un usuario.

Obligación de notificación

Todos los empleados, proveedores o colaboradores que detecten o sospechen un incidente deben **notificarlo de forma inmediata**, sin intentar resolverlo por cuenta propia.

Canales de notificación

Se podrá notificar un incidente a través de los siguientes medios:

- Correo electrónico directo al Responsable de Seguridad o al Comité de Seguridad: seguridad@techsys.com
- Plataforma interna de soporte técnico (ticket de incidente).
- Comunicación directa a un supervisor o al equipo de TI.

> *La notificación debe realizarse lo antes posible, idealmente en menos de 2 horas desde la detección del incidente.*

Información a incluir en la notificación

- Breve descripción del incidente.

- Fecha y hora aproximada de ocurrencia o detección.
- Sistemas, usuarios o dispositivos afectados.
- Cualquier acción realizada antes o después del incidente.
- Evidencias disponibles (capturas, correos, nombres de archivo, etc.).

Gestión posterior

- El equipo de seguridad clasificará el incidente según su **gravedad e impacto**.
- Se activará el protocolo de respuesta correspondiente (ver punto 19).
- Si se confirma que se ha producido una **brecha de datos personales**, se evaluará si es necesario notificar a la **Agencia Española de Protección de Datos (AEPD)** dentro de las 72 horas.

19. Respuesta y mitigación de incidentes

Una vez detectado y notificado un incidente de seguridad, *TechSys Solutions S.L.* debe activar su plan de respuesta para contener, investigar, resolver y aprender del evento. El objetivo es reducir el impacto, recuperar la normalidad operativa y evitar recurrencias.

Fases de la respuesta

1. **Detección y notificación**
   Recepción de la alerta o reporte del incidente según el procedimiento descrito en el punto anterior.

2. **Clasificación del incidente**
   El equipo de seguridad (TI o Comité de Seguridad) evalúa:

   - Tipo de incidente (tecnológico, físico, lógico, humano).
   - Activos afectados.
   - Nivel de impacto y criticidad.

- Urgencia de la respuesta.

3. **Contención inmediata**
    - Aislamiento de sistemas comprometidos (por ejemplo, desconectar de red).
    - Bloqueo de cuentas o servicios afectados.
    - Activación de backups o redundancias si fuera necesario.
4. **Mitigación**
    - Aplicación de parches o medidas de corrección.
    - Eliminación de malware o elementos comprometidos.
    - Revocación de accesos indebidos.
5. **Recuperación**
    - Restauración de sistemas desde copias de seguridad confiables.
    - Revisión de configuraciones.
    - Verificación de integridad de datos.
6. **Análisis y documentación**
    - Recopilación de evidencias técnicas y testimonios.
    - Análisis forense si se requiere.
    - Determinación de la causa raíz.
    - Evaluación de cumplimiento de RTO y RPO.
7. **Informe post-incidente**
    - Elaboración de un informe detallado con:
        - Cronología del incidente.
        - Medidas aplicadas.
        - Lecciones aprendidas.
        - Propuestas de mejora.

Roles y responsables

- El **Departamento de TI** coordina la respuesta técnica.
- El **Responsable de Seguridad** lidera el proceso y comunica al Comité de Seguridad.
- El **DPO**, si aplica, valora la notificación a la AEPD en caso de brecha de datos personales.
- Las áreas afectadas deben colaborar plenamente en todo el proceso.

Comunicación

Dependiendo de la magnitud del incidente, se podrá activar:

- Comunicación interna a los empleados.
- Notificación a clientes, proveedores u otros afectados.
- Notificación a autoridades competentes, si es legalmente exigido.

20. Registro y seguimiento de incidentes

TechSys Solutions S.L. mantiene un registro centralizado de todos los incidentes de seguridad reportados, con el fin de analizarlos, extraer patrones, evaluar su impacto y mejorar los controles preventivos y correctivos.

Objetivos

- Documentar de forma sistemática todos los incidentes, incluso los menores.
- Identificar tendencias o debilidades recurrentes en la seguridad.
- Facilitar auditorías internas y externas.
- Servir como evidencia ante requerimientos legales o regulatorios.
- Medir la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI).

Contenido del registro

Cada incidente debe quedar registrado con, al menos, la siguiente información:

- Identificador único del incidente.
- Fecha y hora de detección y cierre.
- Persona o área que lo reportó.
- Tipo de incidente (por ejemplo: fuga de datos, malware, acceso no autorizado).
- Descripción detallada de lo ocurrido.
- Sistemas o datos afectados.
- Nivel de impacto (bajo, medio, alto).
- Acciones tomadas (contención, mitigación, recuperación).
- Responsables involucrados.
- Conclusiones y medidas preventivas adoptadas.
- Estado del incidente (abierto, en curso, cerrado).

Herramientas de seguimiento

- El registro podrá mantenerse mediante una **herramienta digital interna**, como un sistema de tickets, hoja de control o plataforma SIEM.
- Todos los registros deben estar **protegidos contra alteraciones**, con acceso limitado al equipo de seguridad y a la alta dirección.

Revisión periódica

- El Comité de Seguridad revisará **trimestralmente** el historial de incidentes.
- Se evaluará la **frecuencia, gravedad y causa raíz** de los eventos.
- Se propondrán **acciones de mejora** o reforzamiento de controles donde sea necesario.

21. Programas de formación en seguridad

La concienciación y capacitación del personal es uno de los pilares clave en la estrategia de ciberseguridad de *TechSys Solutions S.L.*. La mayoría de los incidentes de seguridad tienen un componente humano, por lo que es esencial que todos los empleados conozcan los riesgos, buenas prácticas y procedimientos de actuación.

Objetivos

- Promover una **cultura de seguridad** en toda la organización.
- Reducir el riesgo de errores humanos, negligencia o malas prácticas.
- Asegurar que el personal entienda su rol en la protección de la información.
- Cumplir con los requisitos legales y normativos en materia de formación.

Público objetivo

Todos los empleados, sin importar su rol o ubicación, deben participar en actividades de formación. Se establecerán **niveles de profundidad** según el perfil del usuario:

- Nivel básico: personal general.
- Nivel intermedio: usuarios que manejan datos sensibles.
- Nivel avanzado: administradores de sistemas, desarrolladores, equipo de seguridad.

Tipos de formación

1. **Formación inicial (onboarding)**
    - Curso obligatorio para todo nuevo ingreso.
    - Introducción a la política de seguridad, buenas prácticas, uso de contraseñas, correo electrónico seguro, manejo de datos personales.
2. **Formación continua anual**
    - Talleres, webinars o cursos virtuales actualizados.

    - Adaptados a cambios tecnológicos, nuevas amenazas o actualizaciones normativas.

3. **Formación específica por rol**
    - Desarrollo seguro para programadores.
    - Gestión de accesos y backups para TI.
    - Protección de datos personales para atención al cliente, finanzas y RRHH.
4. **Formación reactiva**
    - Reforzada tras un incidente, especialmente para los implicados.

Evaluación y seguimiento

- Se realizarán **evaluaciones de conocimientos** tras las sesiones de formación.
- El área de seguridad llevará un **registro de participación** y resultados.
- Los empleados que no completen la formación obligatoria podrán ver **restringido su acceso** a ciertos recursos hasta regularizar su situación.

22. Campañas de concienciación

Además de los programas formativos, *TechSys Solutions S.L.* desarrollará campañas periódicas de concienciación en seguridad de la información con el fin de reforzar hábitos seguros, mantener la atención frente a amenazas actuales y consolidar una cultura de ciberseguridad en todos los niveles de la organización.

Objetivos

- Generar hábitos cotidianos de protección de la información.
- Sensibilizar sobre los riesgos reales y las consecuencias de un mal uso.
- Reforzar temas clave como phishing, ingeniería social, contraseñas, acceso remoto, privacidad de datos y uso de dispositivos.
- Mantener activa la participación y el compromiso de los empleados con la seguridad.

Formatos y acciones posibles

- **Carteles y mensajes visuales** en oficinas o entornos virtuales (fondos de pantalla corporativos, banners en el portal interno).
- **Boletines informativos** mensuales o trimestrales con consejos de seguridad.
- **Simulacros de phishing** para evaluar y entrenar la capacidad de reacción.
- **Desafíos o trivias** con premios simbólicos (gamificación).
- **Videos cortos** con mensajes clave o actualizaciones de seguridad.
- **Campañas temáticas** (por ejemplo, “Mes de la Ciberseguridad”) con foco en un riesgo específico.

Frecuencia

- Al menos **una acción de concienciación por trimestre**.
- Acciones adicionales en respuesta a incidentes, cambios tecnológicos o campañas externas (como el Mes Europeo de la Ciberseguridad).

Seguimiento

- El Comité de Seguridad supervisará el calendario y el impacto de las campañas.
- Se podrán realizar encuestas breves para medir la percepción y el nivel de compromiso del personal.

23. Evaluación de conocimientos en seguridad

TechSys Solutions S.L. establece mecanismos de evaluación periódica para medir el nivel de comprensión, aplicación y madurez en materia de seguridad de la información entre sus empleados y colaboradores.

Objetivos

- Verificar la **efectividad de la formación y campañas de concienciación**.
- Identificar áreas de mejora o refuerzo formativo por departamento o perfil.
- Asegurar que los usuarios conocen y aplican las políticas de seguridad.
- Garantizar la adecuación del personal a sus responsabilidades frente a la seguridad.

Tipos de evaluación

1. **Evaluación inicial (post-onboarding)**
    - Realizada al finalizar la formación de ingreso.
    - Evalúa comprensión de las normas básicas de seguridad.
2. **Evaluaciones periódicas (anuales o semestrales)**
    - Aplicadas a todo el personal.
    - Se ajustan por nivel de sensibilidad del puesto (básico, intermedio, avanzado).
3. **Evaluaciones específicas tras campañas o incidentes**
    - Sirven para medir el impacto de una campaña puntual (por ejemplo, después de un simulacro de phishing).
    - También pueden usarse tras un incidente para reforzar conceptos clave.

Contenido

- Preguntas de opción múltiple o verdadero/falso.
- Escenarios prácticos (qué harías si…).
- Reconocimiento de prácticas inseguras.

- Identificación de correos maliciosos, políticas internas y acciones correctas.

Herramientas y gestión

- Las evaluaciones se realizarán mediante plataformas internas de e-learning o formularios digitales controlados.
- El Departamento de Seguridad y el Comité de Seguridad harán el seguimiento de los resultados.

Medidas según desempeño

- En caso de bajo rendimiento, se podrá asignar **formación adicional obligatoria**.
- En perfiles críticos (TI, desarrollo, atención al cliente, etc.), se podrá limitar temporalmente el acceso a sistemas sensibles hasta completar la formación requerida.

24. Auditorías internas de seguridad

Las auditorías internas permiten a *TechSys Solutions S.L.* evaluar de forma sistemática el grado de cumplimiento de sus políticas de seguridad, identificar posibles brechas, verificar la eficacia de los controles implementados y garantizar la mejora continua del SGSI (Sistema de Gestión de Seguridad de la Información).

Objetivos

- Comprobar que las políticas y procedimientos de seguridad se aplican correctamente.
- Detectar vulnerabilidades o desviaciones en los controles establecidos.
- Verificar el cumplimiento con normativas aplicables (RGPD, LOPDGDD, estándares ISO, etc.).

- Generar evidencia documentada para auditorías externas o certificaciones.

Alcance

Las auditorías pueden cubrir, entre otros:

- Gestión de accesos y privilegios.
- Seguridad en la red y dispositivos.
- Protección de datos personales.
- Registro y gestión de incidentes.
- Cumplimiento de políticas de uso aceptable.
- Seguridad en el desarrollo de software y pruebas.
- Aplicación de planes de continuidad y respaldo.

Frecuencia

- Se realizará al menos **una auditoría interna completa al año**.
- También se podrán realizar **auditorías parciales o temáticas** de forma trimestral o ante situaciones especiales (por ejemplo, cambios importantes en infraestructura o tras un incidente crítico).

Metodología

- Las auditorías serán realizadas por personal designado del Comité de Seguridad o por un equipo interno con independencia funcional del área auditada.
- Se utilizarán **listas de verificación (checklists)** basadas en las políticas internas y buenas prácticas del sector.
- Las auditorías deberán estar **documentadas en informes firmados**.

Resultados y acciones

- Se generará un **informe de auditoría** con:

    - Hallazgos detectados.
    - Riesgos asociados.
    - Recomendaciones de mejora.
    - Plazos y responsables asignados para la corrección.
- El Comité de Seguridad hará **seguimiento de las acciones correctivas y preventivas** derivadas.

25. Evaluaciones de cumplimiento

TechSys Solutions S.L. lleva a cabo evaluaciones periódicas de cumplimiento con el fin de verificar que sus prácticas, procedimientos y tecnologías se alinean con:

- Las políticas internas de seguridad de la información.
- Las leyes y normativas aplicables (RGPD, LOPDGDD, Ley de Servicios Digitales, entre otras).
- Contratos y acuerdos con clientes, proveedores o terceros.
- Estándares y buenas prácticas (como ISO/IEC 27001).

Objetivos

- Detectar incumplimientos o desviaciones respecto a lo establecido.
- Reducir el riesgo de sanciones legales, contractuales o reputacionales.
- Demostrar compromiso con la protección de la información.
- Asegurar la evolución del SGSI de forma alineada a marcos de referencia actualizados.

Ámbitos de evaluación

- Tratamiento de datos personales y ejercicio de derechos.
- Tiempos y procedimientos de conservación/eliminación de información.
- Seguridad en aplicaciones y desarrollo de software.
- Medidas de protección implementadas en el entorno BYOD y remoto.
- Condiciones de subcontratación (encargados de tratamiento).
- Aplicación de controles de acceso y uso aceptable de recursos.
- Formación y concienciación en seguridad.

Metodología

- Se realizarán mediante entrevistas, revisión de documentación, análisis de registros, y muestreo de controles técnicos.
- El Comité de Seguridad coordinará las evaluaciones, que podrán ser internas o realizadas por consultores externos especializados.
- Las **no conformidades detectadas** se registrarán para su seguimiento.

Frecuencia

- Se realizarán **al menos una vez al año**, y también:
    - Tras cambios importantes en los sistemas.
    - Como preparación para auditorías externas.
    - A raíz de incidentes o requerimientos regulatorios.

Resultados

- Cada evaluación generará un **informe de cumplimiento**, con:
    - Nivel de conformidad por área o control.
    - Recomendaciones de mejora.
    - Plazos para subsanación y responsables asignados.

26. Acciones correctivas y preventivas

TechSys Solutions S.L. establece un proceso estructurado para gestionar acciones correctivas y preventivas que permitan resolver problemas detectados y evitar su recurrencia, como parte de su compromiso con la mejora continua en seguridad de la información.

Objetivos

- Corregir desviaciones, errores o incumplimientos detectados en auditorías, evaluaciones o incidentes.
- Prevenir que se repitan condiciones que puedan comprometer la seguridad.
- Fortalecer el SGSI con base en lecciones aprendidas y buenas prácticas.

¿Cuándo aplicar estas acciones?

Se generarán acciones correctivas o preventivas ante:

- Resultados de auditorías internas o externas.
- Evaluaciones de cumplimiento que detecten no conformidades.
- Incidentes de seguridad, tanto técnicos como organizativos.
- Simulacros o pruebas que evidencien debilidades en los controles.
- Cambios relevantes en los sistemas o normativas aplicables.

Proceso general

1. **Identificación del problema o causa raíz**
    - Análisis de logs, entrevistas, revisión documental, análisis forense.

2. **Clasificación**
    - Se determina si corresponde una acción correctiva (solucionar algo que ya ocurrió) o preventiva (evitar que ocurra en el futuro).
3. **Propuesta de acción**
    - Diseño de medidas técnicas, organizativas o de formación.
    - Asignación de responsables y plazos.
4. **Implementación**
    - Aplicación de la medida con seguimiento desde el Comité de Seguridad.
5. **Verificación de efectividad**
    - Revisión posterior para confirmar que la acción resolvió o previno el problema de forma efectiva.
6. **Documentación**
    - Todo el proceso quedará registrado en el sistema de gestión o en informes del SGSI.

Ejemplos comunes

- Reforzar contraseñas tras una auditoría que detecta claves débiles.
- Realizar formación adicional a un equipo tras caer en un simulacro de phishing.
- Aplicar parches de seguridad tras detectar una vulnerabilidad no mitigada.
- Revisar contratos con proveedores tras incidentes relacionados con terceros.

27. Planificación de la continuidad del negocio

TechSys Solutions S.L. establece una estrategia de continuidad del negocio con el fin de asegurar la disponibilidad de los servicios críticos, incluso ante situaciones de crisis, incidentes graves o desastres que afecten la infraestructura, los sistemas o el personal.

Objetivos

- Garantizar que los procesos clave de la empresa puedan continuar o recuperarse rápidamente tras una interrupción.
- Proteger la integridad y disponibilidad de la información y los servicios ofrecidos.
- Minimizar el impacto económico, reputacional y operativo ante incidentes graves.

Componentes del plan de continuidad

1. **Análisis de impacto en el negocio (BIA)**
    - Identificación de procesos críticos y dependencias tecnológicas.
    - Determinación de RTO (Tiempo Objetivo de Recuperación) y RPO (Punto Objetivo de Recuperación) por sistema o servicio.
2. **Identificación de recursos críticos**
    - Infraestructura tecnológica (servidores, VPN, backups).
    - Personal clave por área funcional.
    - Accesos y comunicaciones remotas (teletrabajo).
3. **Estrategias de recuperación**
    - Uso de copias de seguridad locales y en la nube.
    - Alternativas para acceso remoto y continuidad del soporte al cliente.
    - Redundancia de servicios o infraestructura clave en sede central.
    - Procedimientos para operar en modo degradado si fuera necesario.

4. **Plan de comunicación en crisis**
    - Canales y mensajes definidos para empleados, clientes y autoridades.
    - Voceros asignados y rutas de escalamiento.
5. **Asignación de roles y responsabilidades**
    - Comité de Continuidad o equipo de crisis.
    - Responsables por área operativa y técnica.

Revisión y actualización

- El plan se revisará **al menos una vez al año** o tras cualquier evento significativo (cambio en estructura, incidentes, etc.).
- Se realizarán **pruebas periódicas de simulación** para verificar su eficacia.

28. Recuperación ante desastres

El plan de recuperación ante desastres (Disaster Recovery Plan, DRP) es una extensión específica del plan de continuidad del negocio que define las acciones técnicas necesarias para restaurar los sistemas informáticos y servicios críticos de *TechSys Solutions S.L.* tras un evento disruptivo.

Objetivo

Restaurar la **operatividad tecnológica mínima viable** en el menor tiempo posible tras un desastre natural, ciberataque, fallo masivo de infraestructura o cualquier evento que afecte gravemente a los sistemas de la empresa.

Ámbitos cubiertos

- Servidores físicos y virtuales.
- Sistemas de correo electrónico y VPN.
- Bases de datos críticas (clientes, facturación, proyectos).

- Sistemas de desarrollo y almacenamiento en la nube.
- Equipos de usuarios clave.
- Comunicaciones y acceso remoto.

Estrategias de recuperación

1. **Copia de seguridad y restauración**
    - Backups diarios automatizados (en sede y en la nube).
    - Retención de copias por periodos definidos (por ejemplo, 5 días completos).
    - Pruebas regulares de recuperación para verificar integridad.
2. **Infraestructura alternativa**
    - Posibilidad de operar desde otras sedes o en modalidad 100 % remota.
    - Accesos habilitados vía VPN con MFA desde ubicaciones seguras.
3. **Restauración priorizada**
    - Restauración en orden definido por impacto y dependencia:
        1. Comunicaciones (VPN, correo).
        2. Sistemas de clientes y soporte.
        3. Bases de datos operativas.
        4. Plataformas de desarrollo y trabajo interno.
4. **Equipos de intervención**
    - Equipo de TI con roles asignados para recuperación rápida.
    - Soporte escalado con proveedores externos cuando sea necesario.

RTO y RPO

- **RTO (Recovery Time Objective)**: Tiempo máximo admisible sin servicio.

- **RPO (Recovery Point Objective)**: Pérdida máxima de datos aceptable (en tiempo).

Estos valores se definen por servicio y se documentan en el plan técnico.

Documentación y pruebas

- El DRP estará documentado y **disponible fuera del entorno afectado**.
- Se realizarán al menos **una prueba de recuperación al año** para asegurar la viabilidad del plan.

29. Pruebas y revisión del plan

TechSys Solutions S.L. establece un proceso regular de **pruebas, revisión y mejora** de los planes de continuidad del negocio y recuperación ante desastres, con el objetivo de validar su eficacia y adaptabilidad ante posibles escenarios reales.

Objetivos

- Verificar que los planes funcionan según lo previsto.
- Evaluar la preparación y coordinación del personal involucrado.
- Detectar posibles errores, carencias o mejoras necesarias.
- Asegurar que los tiempos de recuperación (RTO y RPO) se cumplen.
- Actualizar los planes ante cambios en la estructura, tecnología o procesos.

Tipos de pruebas

1. **Simulacros teóricos (tabletop)**
    - Reunión con los equipos clave para repasar roles, decisiones y acciones ante un escenario hipotético.
2. **Pruebas técnicas parciales**

    - Restauración de sistemas, acceso remoto, failover de servidores, verificación de copias de seguridad.

3. **Pruebas completas (mock drill)**

    - Simulación integral de un evento disruptivo que afecta sistemas, comunicaciones y personal.

Frecuencia

- Se realizarán **al menos una vez al año**.
- También se realizarán **tras cambios significativos** en sistemas, proveedores, procesos o estructura organizativa.

Responsables

- El **Comité de Seguridad** y el **Departamento de TI** coordinarán las pruebas.
- Se asignarán observadores o evaluadores para recoger resultados objetivos.

Documentación y mejora

- Cada prueba debe generar un **informe de evaluación**, que incluya:
    - Tiempo de recuperación real.
    - Dificultades encontradas.
    - Nivel de preparación de los participantes.
    - Recomendaciones de mejora.
- Los planes deben actualizarse en base a estos informes.

30. Proceso de revisión periódica

TechSys Solutions S.L. establece un proceso de revisión continua de esta Política de Seguridad de la Información y de todos los documentos que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su adecuación a los riesgos, tecnologías, regulaciones y objetivos del negocio.

Objetivos

- Asegurar que la política y los procedimientos estén **actualizados**.
- Adaptar el SGSI a **cambios organizativos, normativos o tecnológicos**.
- Incorporar las lecciones aprendidas de auditorías, incidentes o pruebas.

Frecuencia de revisión

- La política será revisada al menos **una vez al año**.
- También se revisará de forma extraordinaria cuando ocurra alguno de los siguientes eventos:
    - Cambios significativos en los sistemas o la infraestructura tecnológica.
    - Modificaciones legales o regulatorias aplicables.
    - Incidentes de seguridad graves.
    - Reestructuración de áreas críticas o incorporación de nuevos servicios.

Responsables

- La revisión será coordinada por el **Responsable de Seguridad de la Información**, con la participación del **Comité de Seguridad** y representantes de los departamentos clave.

Resultados

- Cada revisión generará un **informe de actualización**, que incluirá:
    - Cambios propuestos.

    - Motivos de la revisión.
    - Revisión de efectividad de controles existentes.
- Las versiones actualizadas serán **aprobadas por la Dirección** y difundidas según el procedimiento de comunicación de cambios.

31. Actualización y comunicación de cambios

Para mantener la efectividad de su sistema de seguridad, *TechSys Solutions S.L.* establece un procedimiento formal de **actualización, validación y comunicación** de cualquier cambio que afecte esta Política de Seguridad de la Información u otros documentos del SGSI.

Tipos de cambios

- Cambios menores: ajustes de redacción, actualización de responsables, enlaces o nombres.
- Cambios mayores: modificaciones de controles, incorporación de nuevos procedimientos, políticas o tecnologías.

Procedimiento de actualización

1. **Detección de necesidad de cambio**
    - A partir de revisiones, auditorías, incidentes, nueva legislación o recomendaciones del Comité de Seguridad.
2. **Evaluación y propuesta**
    - El Responsable de Seguridad analiza el cambio necesario y redacta una propuesta.
3. **Aprobación**

    - Los cambios deben ser **validados por el Comité de Seguridad** y **aprobados por la Dirección General** antes de su entrada en vigor.

4. **Registro de versiones**

    - Se mantendrá un **historial de versiones** con fecha de publicación, descripción de cambios y responsable.

Comunicación interna

Una vez aprobado un cambio, se deberá:

- Informar a **todo el personal afectado** mediante correo interno, boletines, reuniones o a través de la intranet.

- En caso de cambios relevantes, se podrá requerir **lectura obligatoria y confirmación por parte del usuario**.

- Actualizar las **sesiones de formación o concienciación** si fuera necesario.

Control documental

- La versión vigente estará **disponible en un repositorio oficial**, accesible para todo el personal autorizado.

- Versiones obsoletas deberán ser retiradas y marcadas como “No vigentes”.

32. Aprobación de la política

Esta Política de Seguridad de la Información ha sido elaborada por el **Responsable de Seguridad de la Información**, revisada por el **Comité de Seguridad**, y cuenta con el respaldo y aprobación de la **Dirección General de TechSys Solutions S.L.**.

Con su aprobación, esta política entra en vigor y se considera de **cumplimiento obligatorio para todo el personal**, incluyendo empleados, colaboradores, contratistas y proveedores con acceso a los sistemas o información de la empresa.

Datos de aprobación

- **Versión:** 1.0
- **Fecha de aprobación:**
- **Responsable de la política:** Responsable de Seguridad de la Información
- **Aprobado por:** Dirección General
- **Firma: _____**
- **Nombre y cargo: _____**
- **Lugar:** Madrid