## Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

# ALMACENAMIENTO EN LA RED CORPORATIVA

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | PRO | **Inventario de los servidores de almacenamiento.** Informas a los empleados sobre los servidores de almacenamiento disponibles, la información que se comparte, qué datos deben almacenarse en ellos y las responsabilidades que conlleva. | ☐ |
| B | PRO | **Criterios de almacenamiento.** Informas a los empleados sobre los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimina la información). | ☐ |
| B | PRO | **Clasificación de la información.** Informas al empleado sobre la necesidad de cumplir la política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa. | ☐ |
| A | PRO/TEC | **Control de acceso.** Estableces e implementas reglas de acceso que permiten llevar un control de quién tiene acceso y a qué discos/directorios. | ☐ |
| A | PRO/TEC | **Copias de seguridad.** Defines un plan de copias de seguridad en el que se detalla la información a guardar, cada cuanto tiempo se va a realizar, donde se va a almacenar y el tiempo de conservación de la copia. | ☐ |
| A | TEC | **Acceso limitado.** Permites el acceso a los empleados solo a los repositorios necesarios para el desempeño de su trabajo. | ☐ |
| A | TEC | **Almacenamiento clasificado.** Creas carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Asignas los permisos de acceso pertinentes según el perfil del empleado. | ☐ |
| A | TEC | **Auditoría de servidores.** Revisas periódicamente el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc. | ☐ |
| A | TEC/PER | **Cifrado de la información.** Cifras la información crítica almacenada en los servidores. | ☐ |

# ALMACENAMIENTO EN LA NUBE

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | PRO | **Uso de servicios de almacenamiento en *cloud* públicas.**<br>Informas a los empleados sobre si se permite o se prohíbe el uso de servicios de almacenamiento en *cloud* públicas. | ☐ |
| B | PRO | **Lista de servicios *cloud* permitidos.**<br>Elaboras una lista donde los empleados pueden consultar qué servicios de almacenamiento en *cloud* están permitidos y cuáles no. | ☐ |
| B | PRO | **Proceso de borrado de la información en la nube.**<br>Informas al personal sobre el procedimiento de borrado adecuado para los repositorios de información en la nube. | ☐ |
| B | PRO | **Tipo de información almacenada y tratamiento.**<br>Informas a los empleados del tipo de información que pueden almacenar en la nube y si necesita ser cifrada. | ☐ |
| B | PRO | **Copias de seguridad en la nube.**<br>Valoras las ventajas e inconvenientes antes de almacenar tus copias de seguridad en la nube. | ☐ |
| A | PRO/TEC | **Contratación de servicios de almacenamiento en la nube.**<br>Contratas un servicio de almacenamiento en *cloud* que cumple con los criterios organizativos y obligaciones legales de tu empresa. | ☐ |
| B | PRO/TEC | **Política de seguridad del proveedor.**<br>Conoces la política de seguridad del proveedor de servicios de almacenamiento en la nube. | ☐ |

## APLICACIONES

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | PRO | **Registro de licencias**<br>Mantienes un registro actualizado de las licencias disponibles del software autorizado. | ☐ |
| B | PRO | **Competencia para la instalación, actualización y borrado**<br>Nombras y autorizas al personal técnico que se encargará de la instalación, actualización y eliminación del software de los equipos de la empresa. | ☐ |
| B | PRO | **Sanciones por usos no autorizados**<br>Informas al personal de la empresa de las sanciones derivadas del uso no autorizado de software. | ☐ |
| B | PRO/TEC | **Repositorio de software**<br>Mantienes un repositorio donde se encuentra todo el software autorizado y sus correspondientes credenciales de instalación. | ☐ |
| A | PRO/TEC | **Auditoria de software instalado**<br>Analizas cada _____ que el software instalado en cada uno de los equipos de los usuarios está autorizado y tiene licencia. | ☐ |
| B | PER | **Autorización y licencia del software**<br>Utilizas en todos los dispositivos que utilizas software autorizado y que dispone de las correspondientes licencias de uso. | ☐ |
| B | PER | **Política de copias de software**<br>No realizas copias del software puesto a tu disposición sin el debido consentimiento. | ☐ |

# PAGINA WEB

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| A | PRO/TEC | **Certificado web**<br>Proteges los canales por los que se transmite información sensible (correo electrónico, página web, etc.) mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza. | ☐ |
| B | PRO/TEC | **Desarrollo de terceros**<br>Tienes en cuenta criterios de seguridad en los desarrollos llevados a cabo por terceros. | ☐ |
| A | TEC | **Alojamiento en servidor propio**<br>Disponen de medidas de seguridad en los sistemas de alojamiento propio. | ☐ |
| A | TEC | **Alojamiento en servidor externo**<br>Te aseguras que el alojamiento contratado al proveedor disponga de las medidas de seguridad adecuadas y pactadas. | ☐ |
| B | TEC | **Administración por terceros**<br>Mantienes un registro de la actividad de los administradores externos. | ☐ |
| A | TEC | **Configuración del CMS**<br>Aplicas medidas de seguridad al gestor de contenidos. | ☐ |
| B | TEC | **Acceso al panel de control**<br>Aseguras que las claves de acceso al panel de control sean fuertes y cumplan los criterios de seguridad. | ☐ |
| A | TEC | **Limitación de accesos**<br>Los servidores web se han configurado con un límite de accesos concurrentes para evitar ataques de denegación de servicio. | ☐ |
| B | TEC | **Usuarios por defecto**<br>Eliminas los usuarios por defecto de las herramientas y software que soporta la web. | ☐ |
| B | TEC | **Guardado de registros (*logging*)**<br>Guardas un registro de cualquier interacción con la página durante un período de tiempo conveniente. | ☐ |
| A | TEC | **Comercio electrónico**<br>Si la web dispone de comercio electrónico elaboras una normativa de seguridad que sigue las pautas indicadas en la política de comercio electrónico. | ☐ |
| A | TEC | **Sellos de confianza**<br>Dispones de un sello de confianza que acredita la seguridad del sitio web. | ☐ |
| B | TEC | **Copias de seguridad**<br>Realizas copias de seguridad periódicas de la web. | ☐ |

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| A | TEC | **Auditorias**<br>Se realizan auditorías externas para verificar la seguridad. | ☐ |
| B | TEC | **Software actualizado**<br>Actualizas periódicamente el gestor de contenidos, sus complementos y el software del servidor donde se aloja la web. Estas suscrito a un servicio de avisos de seguridad del fabricante del CMS así como de cualquier otro software que utilices. | ☐ |
| B | TEC | **Protección frente al malware**<br>Instalas antivirus en equipos y servidores. | ☐ |

## RECURSOS HUMANOS

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | PRO | **Cláusulas contractuales**<br>Reflejas en los contratos laborales de tus empleados los aspectos más importantes en materia de ciberseguridad. | ☐ |
| B | PRO | **Acuerdos de confidencialidad**<br>Concretas en acuerdos de confidencialidad la manera de gestionar el acceso a la información más sensible. | ☐ |
| B | PRO | **Revisar las referencias de los candidatos**<br>Revisas las referencias de los candidatos antes de su contratación en aquellos puestos que requieren acceso a información muy confidencial. | ☐ |
| B | PRO | **Plan de formación y concienciación en ciberseguridad**<br>Mantienes concienciada y formada a tu plantilla en aspectos relacionados con la ciberseguridad. | ☐ |
| B | PRO | **Política de sanciones y expedientes**<br>Informas a tus empleados de las sanciones que conlleva el uso negligente de la información de tu empresa. | ☐ |
| B | PRO | **Finalización del contrato**<br>Comunicas a tus empleados las obligaciones que deben cumplir con la información de tu empresa al finalizar su contrato. | ☐ |
| B | TEC | **Concesión autorizada de los permisos de acceso**<br>Concedes los permisos oportunos para garantizar que cada empleado solo accede a la información conveniente. | ☐ |
| B | TEC | **Revocación de permisos de acceso**<br>Eliminas los permisos y cuentas de usuario de los empleados que finalizan su contrato. | ☐ |
| B | PER | **Aceptación de las clausulas y políticas de seguridad de la información**<br>Lees, entiendes y firmas los acuerdos, clausulas y políticas relacionados con la seguridad de la información. | ☐ |
| B | PER | **Aprovechamiento de las sesiones formativas y de concienciación**<br>Participas de manera activa en las sesiones formativas de la empresa en materia de ciberseguridad. | ☐ |

# CONTINUIDAD DEL NEGOCIO

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | PRO | **Determinar el alcance del PCN**<br>Analizas para que activos y procesos debes garantizar la continuidad. | ☐ |
| B | PRO | **Concretar el flujo de responsabilidades**<br>Determinas las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres. | ☐ |
| A | PRO/TEC | **Realización del BIA (Análisis del Impacto en el Negocio)**<br>Elaboras detalladamente el BIA de tu empresa. | ☐ |
| B | PRO | **Definir la política de comunicación y aviso a entidades externas**<br>Defines que tipo de mensajes debe transmitir tu empresa en caso de desastre. | ☐ |
| B | PRO | **Caducidad del PCN**<br>Actualizas el plan de continuidad de negocio de tu empresa cada _____. | ☐ |
| A | PRO/TEC | **Elegir la estrategia de continuidad**<br>Eliges la estrategia de continuidad óptima para tu empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo. | ☐ |
| A | PRO/TEC | **Detallar la respuesta a la contingencia**<br>Detallas los procedimientos y controles específicos a ejecutar ante la aparición de un desastre. | ☐ |
| A | PRO/TEC | **Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio**<br>Pruebas y evalúas cada _____ el plan de continuidad de negocio de tu empresa. | ☐ |