# POLÍTICAS DE SEGURIDAD

## PRIMERA POLÍTICA DE SEGURIDAD: ACTUALIZACIÓN DE SOFTWARE

**1.-Antecedentes:**

No tener actualizado de manera conveniente nuestros equipos y aplicaciones nos hace exponernos a riesgos, robos de datos ya sean credenciales de acceso, datos confidenciales, etc. Hay una cierta necesidad de tener permanentemente actualizados nuestro software, porque todo software tiene un ciclo de vida y en el caso de estar obsoleto también abre una grieta mas de quedarnos sin soporte de fabricante, haciéndonos así un blanco fácil.

**2.-Objetivos:**

Una revisión constante de actualizaciones y parches de seguridad, además de elaborar unos procedimientos que nos permitan instalar estas actualizaciones de manera segura y controlada.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |
| --- | --- | --- |
| **ALCANCE** | **CONTROL** |  |
| TEC | **Determinar cuándo y qué actualizaciones instalar**  Revisa las características y los requisitos de las actualizaciones y parches antes de instalarlos. | ☐ |
| TEC | **Probar las actualizaciones**  Analizas y contrastas en un entorno de pruebas las actualizaciones que deseas instalar. | ☐ |
| TEC | **Deshacer los cambios**  Cuentas con mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente. | ☐ |
| TEC | **Herramientas de diagnóstico y actualización**  Utilizas herramientas de autodiagnóstico para detectar software no actualizado en tus equipos. | ☐ |
| PER | **Configuración de un sistema de alertas**  Tienes configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad. | ☐ |

## SEGUNDA POLÍTICA DE SEGURIDAD: DISPOSITIVOS DE ALMACENAMIENTO

**1.-Antecedentes:**

Los dispositivos de almacenamiento permiten una transferencia rápida y directa de la posible información que tengamos. Hoy en día estos dispositivos son imprescindibles y muy utilizados. Por esto, debemos aplicar unas medidas apropiadas, por ejemplo en el caso de querer almacenar información sensible o confidencial deberemos hacer uso de un dispositivo externo debidamente protegido además de ser corporativo, se almacenará en un lugar seguro y en caso de alguna incidencia se le informará al responsable. Para que podamos asegurar la información contenida en estos dispositivos deberemos aplicar unas medidas de seguridad ya sea por ejemplo cifrar los datos, establecer permisos de acceso e incluso cambiar periódicamente la contraseña.

**2.-Objetivos**

Establecer unas normas del uso de estos dispositivos para garantizar la seguridad de información corporativa que almacena y la de los equipos que se conectan a la misma.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| B | PRO | **Normativa de almacenamiento en dispositivos extraíbles.**  Elaborar una normativa específica para el uso de dispositivos extraíbles (dispositivos autorizados, condiciones de uso, cómo se accede a la información, configuraciones de seguridad, etc.) | ☐ |
| B | PRO | **Concienciación de los empleados**  Involucras a los usuarios en la protección de estos dispositivos y los datos que contienen. | ☐ |
| B | PRO/TEC | **Alternativas a los medios de almacenamiento extraíble.**  Implementar alternativas para evitar la necesidad de utilizar dispositivos de almacenamiento externo (repositorios comunes, *clouds* autorizados, etc.). | ☐ |
| B | TEC | **Registro de usuarios y dispositivos.**  Mantienes un registro actualizado con usuarios, dispositivos y privilegios de acceso. | ☐ |
| B | TEC | **Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en el dispositivo extraíble.**  Aplicar medidas para el almacenamiento seguro de la información en el dispositivo extraíble (cifrado de datos, autenticación, cambio periódico de contraseñas, etc.) | ☐ |

## TERCERA POLÍTICA DE SEGURIDAD:ANTIMALWARE

**1.-Antecedentes**

Aparecen virus constantemente y con ellos otros tipos de malware, estos son una de las principales amenazas a la que se enfrentan nuestros sistemas a dia de hoy. Hay muchas maneras de que nuestro sistema se contagie por malware y el daño que puedan causar hace obligatorio tener un establecimiento de una política de control de malware, teniendo este establecimiento podremos prevenir este software malicioso

**2.-Objetivos**

Proteger nuestro sistema contra la infección por virus o cualquier otro tipo de malware.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| **B** | **PRO** | Instalar o contratar una solución antimalware  Analizas en detalle qué tipo de solución antimalware es la más apropiada para tu empresa y la contratas o la instalas. | ☐ |
| **A** | **TEC** | Configurar las herramientas de detección de malware  Configuras correctamente todas las funcionalidades de tus herramientas de control de malware. | ☐ |
| **B** | **TEC** | Actualizar las herramientas de detección de malware Actualizas cada herramientas de detección y control de malware que tienes instaladas. | ☐ |
| **A** | **TEC** | Establecer el procedimiento de respuesta ante la infección por ejecución de malware  Elaborar procedimientos detallados de actuación ante infecciones por malware. | ☐ |
| **B** | **PER** | Buenas prácticas para el control de malware  Sigues las directrices básicas para prevenir las infecciones por malware. | ☐ |

## CUARTA POLÍTICA DE SEGURIDAD: BORRADO SEGURO Y GESTIÓN DE SOPORTE

**1.-Antecedentes:**

Hay momentos donde la información a veces deja de ser necesaria y llega el momento de deshacerse de ella destruyendo esta de forma segura, esto es indispensable hacerlo si queremos que la información no vuelva a ser accesible. En caso de que esta información no esté en un dispositivo electrónico deberemos hacer uso de una trituradora para deshacernos de esta información, esto nos asegura la destrucción con garantía.

**2.-Objetivos:**

El objetivo es establecer diversas normas de un borrado seguro de información que ya no sea necesaria.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| B | PRO | **Inventario de activos**  Realizas un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio. | ☐ |
| B | PRO/TEC | **Gestión de soportes**  Supervisar los dispositivos que almacenan información corporativa, en particular aquellos que se utilizan para realizar copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc. | ☐ |
| A | PRO/TEC | **Eliminación de la información en soportes no electrónicos**  Utilizas el proceso de triturado para destruir la información de los soportes no electrónicos (papel y soportes magnéticos). | ☐ |
| A | PRO/TEC | **Eliminación de la información para la reutilización de soportes electrónicos**  Optas por el proceso de sobrescritura cuando quieres reutilizar un soporte todavía en buen estado. | ☐ |
| A | PRO/TEC | **Eliminación de la información antes de deshacernos de soportes electrónicos**  Usas el proceso de desmagnetización o de destrucción física antes de desechar el soporte de almacenamiento. | ☐ |

## QUINTA POLÍTICA DE SEGURIDAD: CONTRASEÑAS

**1.-Antecedentes:**

Para hacer un tratamiento diario de información siempre se requiere un acceso a distintos servicios, ya sean dispositivos o aplicaciones se suelen utilizar unas credenciales como el usuario y contraseña. Para nuestra seguridad se utilizan estas credenciales de autenticación y tenemos que asegurarnos de que se generen, actualicen y funcionen de una forma segura y óptima.

**2.-Objetivos:**

Establecer y verificar el cumplimiento de un uso óptimo de las contraseñas.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** | |
| A | PRO/TEC | **Gestión de contraseñas**  Defines un sistema de gestión de contraseñasavanzado que contempla todos los aspectos relativos a su ciclo de vida. | ☐ |
| A | PRO/TEC | **Técnicas de autenticación externas**  Consideras la utilización de sistemas de autenticación externos descentralizados. | ☐ |
| A | TEC | **Herramientas para garantizar la seguridad de las contraseñas**  Te ayudas de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas. | ☐ |
| B | TEC | **No utilizar las contraseñas por defecto**  Cambias las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones y sistemas. | ☐ |
| B | TEC | **Doble factor para servicios críticos**  Incorporas sistemas de autenticación multifactor en los accesos a servicios con información muy sensible. | ☐ |
| B | PER | **No compartir las contraseñas con nadie**  Mantienes en secreto tus claves y evitas compartirlas. | ☐ |
| B | PER | **Las contraseñas deben de ser robustas**  Generas tus contraseñas teniendo en cuenta su fortaleza. | ☐ |
| B | PER | **No utilizar la misma contraseña para servicios diferentes**  Te aseguras de elegir distintas contraseñas para cada uno de los servicios que utilizas. | ☐ |

## SEXTA POLÍTICA DE SEGURIDAD: COPIAS DE SEGURIDAD

**1.-Antecedentes:**

Los medios de almacenamiento que usamos a nuestro día a día contienen siempre nuestra información, estos medios pueden sufrir una situación como: robos, incendios, inundaciones, roturas, fallos, virus, borrados accidentales, etc. Por ello tener Copias de Seguridad/Backups, es muy importante para mantener bien conservada la información.

**2.-Objetivos:**

Verificar que se hayan realizado copias de seguridad para garantizar un funcionamiento continuo y óptimo del negocio.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| B | PRO | **Inventario de activos de información**  Mantienes un inventario de activos de información  (software, datos, soportes, responsables, ubicación…) y los clasificas para identificar los necesarios (críticos) para reanudar el negocio en caso de desastre o incidente grave. | ☐ |
| B | PRO | **Control de acceso**  Controlas el acceso a las copias de seguridad (sólo personal autorizado). | ☐ |
| B | PRO/TEC | **Copias de seguridad de la información crítica**  Haces copias de seguridad de la información crítica corporativa, la exigida por la ley y la establecida en los contratos. | ☐ |
| B | PRO/TEC | **Periodicidad de las copias de seguridad**  Las copias de seguridad se realizan cada \_\_\_\_\_\_\_\_\_\_. | ☐ |
| B | PRO/TEC | **Tipo de copia apropiada**  Haces copias de seguridad completa, incremental o diferencial (elegir la adecuada para tu empresa). | ☐ |
| B | PRO/TEC | **Caducidad de las copias de seguridad**  Conservas las copias de seguridad durante \_\_\_\_\_\_\_\_\_\_. | ☐ |

## SÉPTIMA POLÍTICA DE SEGURIDAD: USO DEL WIFI Y REDES EXTERNAS

**1.-Antecedentes:**

La empresa debe establecer unas condiciones y circunstancias en las que permita un acceso remoto para determinar quién puede acceder a qué,cómo y cuándo. Una de las herramientas que existen para poder controlar esta seguridad es la utilización de una Red Privada Virtual o VPN. Para acceder a esta información de manera remota se utilizará una VPN. Además de esto hacer un uso de VPN ofrece unas ventajas interesantes, por ejemplo:

·Toda la información se transmite de manera segura

·Confidencialidad e integridad de información ya que está cifrada

·La información solo se transmite entre dispositivos autorizados y configurados para este fin

·Restricción de acceso ya que necesita una previa de autorización

**2.-Objetivos:**

El objetivo principal es poder garantizar una seguridad de los datos y comunicaciones cuando el acceso fuera de las instalaciones se deba llevar a cabo.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL ALCANCE CONTROL** | | |  |
| B | PRO/TEC | **Política de conexión**  Elaboras una normativa corporativa para regular las conexiones externas. | ☐ |
| A | TEC | **Configuración de la VPN**  Configuras una conexión VPN para acceder desde el exterior. Creas cuentas de usuario con permisos de acceso. Detallas el software permitido para realizar estas conexiones. Estableces un tiempo de desconexión automática de la VPN tras un periodo de inactividad. | ☐ |
| B | PER | **Uso de la VPN**  Conoces cómo conectarte vía VPN (si la empresa lo permite) y en qué situaciones debes hacerlo. | ☐ |
| B | PER | **Acceso a redes wifi ajenas**  Al conectarte a una nueva red inalámbrica, compruebas que utiliza el protocolo WPA2.  Compruebas que los sitios a los que accedes tienen certificado y utilizan protocolos seguros (https://) si vas a realizar actividades críticas. | ☐ |
| A | PER | **Configuración de la wifi doméstica**  Antes de utilizarlas, configuras el protocolo WPA2, y cambias el nombre del SSID y las credenciales por defecto. | ☐ |

## OCTAVA POLÍTICA DE SEGURIDAD: CORREO ELECTRÓNICO

**1.-Antecedentes:**

El correo electrónico es uno de los métodos de comunicación más utilizados en las empresas además de otro ámbitos, sus beneficios son bastante evidentes ya sea por accesibilidad, rapidez, posibilidad de enviar documentos aun que no de demasiado peso, poder contactar con varios usuarios al mismo tiempo, etc. Debido a ser una herramienta con la posibilidad de ser utilizado en una corporación debe mantener un control y unas normas específicas de su uso.

**2.-Objetivos:**

Establecer unas normas de uso permitido y seguro del correo electrónico corporativo que sirva para impedir errores, incidentes y usos ilícitos además para evitar ataques por esta vía de comunicación

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| B | PER | **Uso apropiado del correo corporativo** Nunca usas el correo corporativo con fines personales y el contenido cumple las normas marcadas por la empresa. | ☐ |
| B | PER | **Contraseña segura**  Usas una contraseña segura para acceder al correo electrónico. | ☐ |
| B | PER | **Correos sospechosos**  Sospechas de la autenticidad del correo cuando el mensaje presenta cambios de aspecto, contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual o solicita credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.). | ☐ |
| B | PER | **Identificación del remitente**  Identificas los remitentes antes de abrir un correo electrónico. Si sospechas que ha sido suplantado contactas con el remitente por otro medio para confirmarlo. | ☐ |

## NOVENA POLÍTICA DE SEGURIDAD: PROTECCIÓN DE LA PÁGINA WEB

**1.-Antecedentes:**

Es quizás una necesidad tener una página web para dar a conocer cualquier cosa no solo una empresa, por ello. Conociendo este punto, debería tener una seguridad aceptable como para mantener estable una página web.

**2.-Objetivos:**

Proteger nuestra página web de posibles ataques y garantizar una oportuna protección de los datos personales a nuestros usuarios.

**3.-Lista de Control:**

La lista de control va a ser utilizada con el fin de cumplir la política de seguridad en las actualizaciones de software.

Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles

Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables.

Este Control se clasificará en niveles de alcance, es decir que personal o dirección deberá ejercer dicho objetivo de la lista:

·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.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** |  |
| **A** | **TEC** | **Limitación de accesos**  Los servidores web se han configurado con un límite de accesos concurrentes para evitar ataques de denegación de servicio. | ☐ |
| **B** | **TEC** | **Usuarios por defecto**  Eliminas los usuarios por defecto de las herramientas y software que soporta la web. | ☐ |
| **B** | **TEC** | **Guardado de registros (*logging*)**  Guardas un registro de cualquier interacción con la página durante un período de tiempo conveniente. | ☐ |
| **A** | **TEC** | **Comercio electrónico**  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**  Dispones de un sello de confianza que acredita la seguridad del sitio web. | ☐ |
| **B** | **TEC** | **Copias de seguridad**  Realizas copias de seguridad periódicas de la web. | ☐ |
| **A** | **TEC** | **Auditorias**  Se realizan auditorías externas para verificar la seguridad. | ☐ |
| **B** | **TEC** | **Software actualizado**  Actualizas periódicamente el gestor de contenidos, sus complementos y el software del servidor donde se aloja la web. Estás 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**  Instalas antivirus en equipos y servidores. | ☐ |