Medidas de Seguridad

DoctorSender smart

Índice

1. Obligaciones de los usuarios con acceso a datos de carácter personal

- Acceder solo a datos necesarios para sus obligaciones laborares.
- No destruir o alterar datos sin autorización.
- No copiar o comunicar datos a terceros sin autorización.
- Comunicar y subsanar errores en datos.
- Salvaguardar y no revelar el nombre de usuario y contraseña asignados. No usar estos datos fuera de los locales de la empresa
- No realizar transmisiones de datos por Internet sin autorización.
- En departamentos de atención al público, no revelar datos personales sin autorización. Comprobar en todo caso la identidad de quien solicita los datos.
- Si se imprimen documentos en papel, no permitir el acceso a personas no autorizadas.

2. Medidas Organizativas

2.1 Política de seguridad

Existe una política de seguridad formada, además de por este documento, por los siguientes:

- Las normas de uso de los recursos y sistemas de información
- El procedimiento para la gestión de brechas de seguridad.
- El plan de contingencia para los sistemas y servicios de tratamiento
- Los siguientes documentos para el cumplimiento de medidas de seguridad:
- El compromiso de confidencialidad y seguridad
- El documento de recibo de contraseñas y la definición de perfiles y permisos de acceso.
- El documento de entrega de equipos portátiles, en su caso.

2.2 Roles y responsabilidades

Del mismo modo se ha nombrado un responsable de la seguridad y responsables de los recursos que tratan la información personal.

2.3 Política de control de acceso

Cada usuario o proceso que accede al sistema cuenta con un identificador singular de tal forma que se puede saber quién recibe y qué derechos de acceso recibe y quién ha hecho algo y qué ha hecho.

Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibe una identificación singular cada uno de los casos de forma que siempre queden delimitados privilegios y, en su caso, los registros de actividad.

Las cuentas de usuario están asociadas a un identificador único, se inhabilitan cuando el usuario deja la organización, cesa en la función para la cual se requería la cuenta o cuando la persona que la autorizó da orden en sentido contrario y se retienen durante el periodo de retención necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas.

Los derechos de acceso de cada recurso se establecen según las decisiones del responsable del recurso y se revisan periódicamente para comprobar que los permisos concedidos a los usuarios son los adecuados a su perfil.

Los derechos de acceso de cada usuario se asignan atendiendo a los principios de mínimo privilegio, que reduce el acceso al mínimo estrictamente necesario, de necesidad de conocer, que limita el acceso a aquella información requerida para cumplir sus obligaciones y de capacidad de autorizar, que solo el responsable competente puede conceder, alterar o autorizar el acceso. En concreto, se separan al menos las siguientes funciones desarrollo, configuración y mantenimiento y auditoría

3. Gestión de recursos y gestión de cambios

Existe un inventario actualizado de todos los activos asociados a la información personal y a los recursos para el tratamiento de la información, detallando su naturaleza e identificando a su responsable, es decir, la persona que es responsable de las decisiones relativas al mismo. El inventario se mantiene actualizado.

Todos los cambios anunciados por el fabricante o proveedor se analizan para determinar su conveniencia para ser incorporados o no.

Antes de poner en producción una nueva versión o una versión parcheada, se comprueba en un equipo que no esté en producción que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban. Los cambios se planifican para reducir el impacto sobre la prestación de los servicios afectados.

Se dispone de un listado de aplicaciones que deben mantenerse actualizadas y de un procedimiento y unas alertas para analizar, priorizar y determinar cuándo se deben aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones, así como un registro de las actualizaciones y parches instalados.

4. Gestión de Personal

4.1 Deber de confidencialidad y seguridad

Todo el personal con acceso a los datos personales tiene conocimiento de sus obligaciones en materia de seguridad de la información, suscribiendo un documento de confidencialidad y seguridad y protección de datos.

4.2 Formación y sensibilización

Se realizan las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

Se forma regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a la configuración de sistemas, la detección y reacción a incidentes y el almacenamiento, transferencia, copias, distribución y destrucción de soportes con información personal.

5. Respuesta ante incidentes y continuidad de negocio

5.1 Gestión de incidentes y brechas de seguridad

En el caso de que se produzca una brecha de seguridad, el responsable debe valorar si esta supone la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Todos los empleados deben poner en conocimiento del responsable del tratamiento aquellas brechas de seguridad que afecten a datos personales para que este pueda notificarla a la Agencia Española de Protección de Datos, y en su caso a los interesados, en los términos descritos en el apartado Directrices para la gestión de brechas de seguridad de este documento.

Además, y de forma independiente a la notificación de brechas, el responsable tiene implementados los mecanismos necesarios de registro, documentación y gestión de incidentes.

5.2 Definición de un plan de continuidad de negocio

Para el caso de producirse un incidente que pueda suponer la destrucción, pérdida o alteración accidental o ilícita de datos personales que afecte a sistemas o procesos de mayor criticidad se ha definido un plan de continuidad o contingencia que permite recuperar en un plazo razonable la operativa habitual con el fin de garantizar la continuidad del negocio.

6. Medidas Técnicas

6.1 Mecanismo para el control de acceso

6.1.1 Identificación y autenticación de usuarios

El control de acceso a cualquier recurso del sistema para realizar una determinada acción está establecido mediante la identificación y autenticación.
Los recursos del sistema se protegen mediante un mecanismo que impide su utilización salvo que se disfrute de derechos de acceso suficientes.
Los derechos de acceso de cada recurso se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

Las credenciales o contraseñas se activan una vez están bajo el control efectivo y exclusivo del usuario después de reconocer que las ha recibido y aceptar las obligaciones de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida que implica su tenencia.

Las credenciales o contraseñas se deben cambiar al menos con una periodicidad anual y se retiran y son deshabilitadas cuando el usuario, el equipo o el proceso que autentica terminan su relación con el sistema.

El número de intentos permitidos está limitado, bloqueando la oportunidad de acceso una vez efectuados tres números de fallos consecutivos.

Las características mínimas que deberán tener las contraseñas son:

- Tener un mínimo de ocho caracteres.
- Utilizar cadenas de caracteres en las que se mezclen símbolos alfabéticos y numéricos.
- Se deberá cambiar su contraseña, como mínimo cada 6 meses y no se podrá repetir las últimas 3 contraseñas empleadas.
- No se mantendrán escritas las contraseñas en ningún sitio que las haga visibles

Los cambios de personal implicarán el cambio de las contraseñas de todos los equipos, servicios y sistemas a los que el personal saliente tuviera acceso
La cuenta de administrador está en manos del responsable de seguridad y cambiada cada vez que por razones técnicas deba ser conocida por otra persona del servicio técnico.

6.2 Monitorización de los accesos

6.2.1 Registro de actividad de los usuarios

Se registran las actividades de los usuarios en el sistema, de forma que se indica quién realiza la actividad, cuándo la realiza y sobre qué información y si las actividades realizadas con éxito como los intentos fracasados... En el registro también se incluye la actividad de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

Se revisan los registros de actividad buscando patrones anormales.

7. Seguridad de los Datos.

7.1 Protección frente a códigos dañinos

Se dispone de mecanismos de prevención y reacción frente a código dañino (Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como “spyware, y en general, todo lo conocido como “malware”) con mantenimiento de acuerdo a las recomendaciones del fabricante mediante una suite de seguridad que proporciona seguridad integral mediante antivirus, antispam (programa para evitar correos basura), anti-phishing (programa para protegerse contra intentos de intrusión) y si es posible anti-ransomware (Secuestro del ordenador (imposibilidad de uso) o cifrado de sus archivos y promesa de liberarlo mediante pago). Nunca usan antivirus gratuitos y no se instalan dos antivirus de forma simultánea y están correctamente instalados, actualizados y con todos los módulos imprescindibles activados.

7.2 Seudonimización

Está previsto pseudonimizar las categorías especiales de datos personales de manera que ya no pueda atribuirse a un interesado sin utilizar información adicional que figure por separado.

8. Seguridad de las comunicaciones.

8.1 Conexión segura

El router está configurado del modo siguiente:

- Se cambia la clave de acceso a la parte de configuración
- Se mantiene un control de las conexiones
- Se dejan abiertos solamente aquellos puertos que sean imprescindibles, cerrando el resto.
-

Se cambia la configuración de la tecnología que permite la interconexión inalámbrica de dispositivos electrónicos (wi-fi) que tiene por defecto, activando los sistemas de cifrado enrutadores y puntos de acceso, eligiendo como algoritmo de seguridad WPA (Sistema para proteger redes inalámbricas). Se establecerán contraseñas seguras de acceso

8.2 Cortafuegos

Está instalado un cortafuegos (Sistema de protección que evite conexiones no autorizadas, generalmente implementado en el router o dispositivo que implemente esta función) y cambiada la configuración que trae por defecto por otra más restrictiva y se mantiene activo.

8.3 Cifrado de las comunicaciones

Cuando se comuniquen a terceras categorías especiales de datos personales, como por ejemplo datos de salud, se cifran los datos para evitar accesos no autorizados.

8.4 Segmentación de redes

Se acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren. La red se segmenta en segmentos de forma que existe:

- Control de entrada de los usuarios que llegan a cada segmento.
- Control de salida de la información disponible en cada segmento.
- Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado

9. Copias de seguridad

9.1 Copias y procedimiento de recuperación

Se realizan copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una periodicidad al menos semanal. Se comprueba periódicamente la correcta realización de copias y la posibilidad de recuperación. Se etiquetan los soportes para realizar las copias de seguridad y se lleva un registro de los soportes sobre los que se ha realizado alguna copia.

Las copias de respaldo disfrutan de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

9.2 Copias y procedimientos de recuperación en otra ubicación

Se realizan copias en un sistema de almacenamiento independiente del propio servidor en el que se ubican los datos, fuera de las instalaciones.

10. Dispositivos Portátiles.

Los equipos corporativos móviles que sean susceptibles de salir de las instalaciones de la organización disponen de las siguientes medidas de protección específicas:

- Existe un procedimiento de solicitud y asignación de los dispositivos móviles corporativos en el que se establece qué se puede almacenar en los equipos corporativos y dónde guardar la información generada en su trabajo dentro del árbol de directorios del equipo.
- Existe un control de acceso mediante autenticación y contraseña y cambio periódico de contraseñas. Se evita que el equipo contenga claves de acceso remoto a la organización capaces de habilitar un acceso a otros equipos de la organización.
- Se informa a los usuarios sobre el cuidado en el uso de dispositivos móviles en zonas públicos, salas de reunión y otras áreas desprotegidas. Existe un canal de comunicación para informar de pérdidas o sustracciones al servicio de gestión de incidentes
- Cuando se conecta a través de redes fuera del control de la organización se requiere autorización previa de los responsables de la información y los servicios afectados y la información y los servicios accesibles se limita a los mínimos imprescindibles.
- Las categorías especiales de datos o sobre personas vulnerables almacenadas en el disco se protegen mediante cifrado.
- Los equipos móviles que no sean corporativos que sean susceptibles de salir de las instalaciones de la disponen de las siguientes medidas de protección específicas:
- Existe un procedimiento en el que se indica a los usuarios que deben separar el uso con fines privados respecto a los del negocio, incluyendo el uso de software para permitir dicha separación y renuncia a la propiedad de los datos de negocio y la limpieza de datos al terminar la relación profesional.
- Se configura el bloqueo automático del dispositivo tras un periodo de inactividad y un control de acceso a la red corporativa (autenticación con contraseñas, doble factor, VPN…)

11. Desarrollo Seguro

11.1 Requisitos de seguridad de equipos y aplicaciones

Se atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas y se efectúa un seguimiento continuo de los anuncios de defectos.

Previamente a su entrada en operación los equipos se configuran de forma que:

- Se retiran cuentas y contraseñas estándar.
- Se aplica la regla de "mínima funcionalidad" proporcionando únicamente la funcionalidad para el desempeño de la función sin funciones gratuitas, ni de operación, ni de administración, ni de auditoría.

- Se crean carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Se asignan los permisos de acceso pertinentes según el perfil del empleado
- Se elimina o desactiva mediante el control de la configuración aquellas funciones que no sean de interés o necesarias o sean inadecuadas al fin que se persigue.
- Se aplica la regla de "seguridad por defecto": protegiendo al usuario por defecto, salvo que se exponga conscientemente a un riesgo, para reducir la seguridad, el usuario tiene que realizar acciones conscientes. El uso natural es un uso seguro.

Se mantiene un registro actualizado de las licencias disponibles del software autorizado y un repositorio donde se encuentra todo el software autorizado y sus correspondientes credenciales de instalación. No se instalan más programas que los necesarios o que no estén relacionados con los servicios que se prestan. Siempre se instalan programas desde fuentes seguras, evitando descargar aplicaciones desde repositorios generalistas.

12. Destrucción de la Información. Reutilización y destrucción de soportes

Si se pretende reutilizar un soporte se deberá impedir la recuperación de la información almacenada anteriormente mediante su formateo. Los soportes que no se vayan a reutilizar deberán ser destruidos de forma segura mediante incineración o triturado.

Si se utiliza un servicio de destrucción deberá disponer de destrucción certificada para garantizar la destrucción segura de soportes con categorías especiales de datos.

13. Medidas de Seguridad Física

13.1 Áreas específicas protegidas

Los sistemas de información críticos y sus componentes están instalados en áreas separadas específicas para su función.
Se controlan los accesos de forma que sólo se puede acceder por las entradas previstas y vigiladas. Se identifica a todas las personas que accedan y se registran sus entradas y salidas.

13.2 Sala de servidores con elementos de protección

Se dispone de elementos adecuados para el eficaz funcionamiento del equipamiento instalado y en especial de condiciones de temperatura y humedad y protección de cableado. Además disponen de la energía eléctrica y sus tomas correspondientes necesaria para su funcionamiento, de forma que se garantiza el suministro de potencia eléctrica y el correcto funcionamiento de las luces de emergencia. También están instalados y mantenidos en perfecto estado extintores para la protección de incendios.

Se dispone de instalaciones alternativas con las mismas garantías de seguridad para poder trabajar en el caso de que las instalaciones habituales no estén disponibles

13.3 Protección de los equipos fijos

Los equipos están situados de tal manera que se minimizan los accesos innecesarios a las áreas de trabajo y están instalados donde se reduce el riesgo de que la información sea vista durante su uso por personas no autorizadas.
El equipo de sobremesa está configurado de tal modo que se bloquea al cabo de un tiempo de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad.
Se exige que los puestos de trabajo permanezcan despejados sin más documentos o soportes encima de la mesa que los requeridos para la actividad que se está realizando en cada momento. Estos documentos y soportes se guardan en lugar cerrado cuando no se están utilizando.

13.4 Almacenamiento de soportes

Existen armarios y archivadores provistos de cerradura y llave para el correcto almacenamiento de documentos y soportes protegiendo y controlando su acceso.

13.5 Tránsito de soportes

Se registra la entrada y salida de los soportes que contienen información personal Durante el transporte deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
Deberá emplearse un servicio fiable de transporte o mensajería y el embalaje deberá proteger suficientemente el contenido de todo daño físico durante el tránsito.

14. Captación de imágenes con cámaras y finalidad de seguridad

En el caso de los sistemas de videovigilancia:

- UBICACIÓN DE LAS CÁMARAS: Se evita la captación de imágenes en zonas destinadas al descanso de los trabajadores.

- UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubican en un espacio de acceso restringido de forma que no sean accesibles a terceros.

- CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenan durante el plazo máximo de un mes, con excepción de las imágenes que debieran aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

- DEBER DE INFORMACIÓN: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo.

- CONTROL LABORAL: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- DERECHO DE ACCESO A LAS IMÁGENES: Para dar cumplimiento al derecho de acceso de los interesados se solicitará el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso

de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

15. Atención del ejercicio de derechos

El responsable del tratamiento informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) y teniendo en cuenta lo siguiente:

Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión), oposición, portabilidad y limitación del tratamiento. El ejercicio de los derechos es gratuito.

- El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida y de forma concisa, transparente, inteligible, con un lenguaje claro y sencillo y conservar l)a prueba del cumplimiento del deber de responder a las solicitudes de ejercicio de derechos formuladas.
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Las solicitudes deben responderse en el plazo de 1 mes desde su recepción, pudiendo prorrogarse en otros dos meses teniendo en cuenta la complejidad o el número de solicitudes, pero en ese caso debe informarse al interesado de la prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

16. Verificación de medidas de seguridad

Se establece una periodicidad anual para realizar los análisis de riesgos respecto a las medidas de seguridad.