Instrucción Seguridad para RGPD

Instrucción de Seguridad para tratamientos de datos personales

Universidad
Carlos III de Madrid
www.uc3m.es

Delegado de Protección de Datos y Responsable de Seguridad de la Información

web: www.uc3m.es

Control de versiones

Fecha	Cambios	Autor	Aprobador
	Versión inicial	DPD, CISO	DPD, CISO

Índice

Objetivo

La presente instrucción pretende ser el marco de referencia que deben cumplir aquellos empleados o encargados de tratamiento para la realización de la labor encomendada por la Universidad Carlos III en lo referente a la Seguridad y Protección de la Información y de los datos personales.

Los objetivos que pretende son minimizar los riesgos en base a las diferentes dimensiones de seguridad:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad
- Trazabilidad

Y la protección de los derechos y libertades de los titulares de los datos personales.

Medidas de protección

Relacionadas con el tratamiento de los datos

mp.td.1 Anonimización

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran confidencialidad de los datos tratados.

Ámbito

Aplica a todos aquellos tratamientos que puedan realizarse sin que sea necesario identificar los datos correspondientes a un único individuo.

Implementación

El procedimiento consiste en eliminar los datos personales que permitan la identificación del titular de los mismos. El Delegado de Protección de Datos y el Responsable de Seguridad determinarán si el procedimiento de anonimización propuesto cumple con los requisitos necesarios que garanticen dicha anonimización.

Implicaciones

Esta medida impedirá correlar informaciones correspondientes al mismo titular, ya que no habrá atributos o información que permita agrupar datos.

mp.td.2 Pseudonimización

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran confidencialidad de los datos tratados.

Ámbito

Aplica a todos los tratamientos que puedan realizarse sin que sea necesario identificar al titular de los mismos.

Implementación

El procedimiento consiste en sustituir los datos identificativos del titular de los datos por un identificador aleatorio, de modo que se puedan agrupar los datos de un individuo determinado. El Delegado de Protección de Datos y el Responsable de Seguridad determinarán si el procedimiento de pseudonimización propuesto cumple con los requisitos necesarios que garanticen dicha pseudonimización.

Implicaciones

Deberá custodiarse adecuadamente los datos y la información que permitan revertir la pseudonimización.

Relacionadas con el equipamiento informático

mp.ei.1 Cifrado del dispositivo

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran confidencialidad de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se pueda tener acceso a dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones, discos USB, etc.

Implementación

El Área de Seguridad y el Centro de Atención a Usuarios establecerán los mecanismos adecuados a cada dispositivo.

Implicaciones

El cifrado del dispositivo dificultará la recuperación de ficheros borrados accidentalmente y/o de soportes dañados, por lo que deberá implementarse un mecanismo alternativo que garantice la disponibilidad de los datos. No está permitida la sincronización automática de datos con los servicios en la nube (Google Drive) y no deberán utilizarse otros sistemas de sincronización sin la aprobación por escrito del Responsable de Seguridad de la Información.

mp.ei.2 Antivirus

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran disponibilidad y/o confidencialidad de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se puedan tratar dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones.

Implementación

El Área de Seguridad y el Centro de Atención a usuarios determinarán el programa antivirus adecuado para el dispositivo..

Implicaciones

Ninguna.

mp.ei.3 Cortafuegos local

Motivación

Esta medida aplica a todos aquellos tratamientos de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se puedan tratar dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones.

Implementación

Por defecto, los dispositivos no serán accesibles desde de la red de datos. En caso de que fuera necesario su acceso a través de la red de datos, contarán con el cortafuegos determinado por el Área de Seguridad y el Centro de Atención de Usuarios y con la configuración que limite el acceso a los servicios exclusivamente necesarios. Los accesos deberán contar con sistemas de autenticación adecuados.

Implicaciones

Siempre que sea posible la configuración del cortafuegos será gestionada de forma centralizada, en el caso de smartphones/tablets mediante el sistema de gestión de dispositivos móviles (MDM).

mp.ei.4 Control de accesos

Motivación

Esta medida aplica a todos aquellos tratamientos de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se puedan tratar dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones.

Implementación

Los dispositivos contarán con sistemas de autenticación que impidan el acceso no autorizado a los mismos.

- Smartphones y tablets, se podrá optar con bloqueos basados en patrones de puntos si lo permite la configuración de cifrado del dispositivo.
- Ordenadores, deberán contar con usuarios de administración y usuarios no privilegiados. Debiendo iniciarse sesión siempre como usuario no privilegiado.

Implicaciones

Siempre que sea posible la configuración del cortafuegos será gestionada de forma centralizada, en el caso de smartphones/tablets mediante el sistema de gestión de dispositivos móviles (MDM).

mp.ei.5 Trabajo con ficheros alojados en el dispositivo

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran disponibilidad de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se puedan tratar dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles.

Implementación

La utilización de dispositivos de almacenamiento locales (discos de equipos de sobremesa, portátiles, discos USB) para almacenamiento de datos personales no se recomienda, ya que impiden o dificultan la creación de copias de respaldo. Por ello se recomienda la utilización del servicio de Google para la edición de documentos (Google Docs, Sheets, etc).

Implicaciones

El Servicio de almacenamiento de datos de Google (Google Drive) se encuentra adherido al "Escudo de privacidad/Privacy Shield" que aporta las garantías necesarias para el almacenamiento de datos personales cumpliendo con el Reglamento General de Protección de Datos (RGPD).

mp.ei.6 Bloqueo de Sesión

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran confidencialidad de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se pueda tener acceso a dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones, etc.

Implementación

Se activará el bloqueo de la pantalla transcurrido un período de tiempo razonable, no superior a 5 minutos.

Implicaciones

Ninguna.

mp.ei.7 Registro de actividad

Motivación

Esta medida aplica a todos aquellos tratamientos de los datos tratados.

Ámbito

Aplica a todos los dispositivos desde los que se puedan tratar dichos datos, esto es, ordenadores de sobremesa/despacho, portátiles, tablets, smartphones.

Implementación

Los dispositivos deberán registrar, en la medida de sus posibilidades, los accesos al sistema. Adicionalmente, si fuera posible, dichos registros se remitirán también al Área de Seguridad y Comunicaciones, para su tratamiento de forma centralizada.

Implicaciones

Ninguna.

Relacionadas con los servicios en la nube

mp.sn.1 Autenticación robusta

Motivación

Esta medida aplica a todos aquellos tratamientos que requieran confidencialidad de los datos tratados.

Ámbito

Aplica los servicios ofrecidos por Google, especialmente al servicio de almacenamiento en la nube (Google Drive), correo electrónico (GMail) y edición de documentos (Google Docs).

Implementación

Deberá activarse la autenticación mediante doble factor de autenticación en todas las cuentas que almacenen datos personales.

Implicaciones

La utilización del segundo factor de autenticación requiere de la utilización de un dispositivo (token) desde el que se genera el segundo factor. Dicho token puede ser una aplicación en el smartphone o un token físico.

Relacionadas con los soportes en papel

RECOMENDACIÓN GENERAL.

Se recomienda con carácter general trabajar con datos personales en soporte electrónico, de modo que la utilización del soporte en papel sea residual y limitada a los supuestos estrictamente necesarios.

mp.sp.1 Guarda y archivo de la documentación bajo llave.

Motivación

Esta medida resulta de aplicación para todos los documentos que contengan datos personales.

Ámbito

La documentación en soporte papel que contenga datos personales debe guardarse y custodiarse bajo llave siempre que no se estén utilizando y tratando.

A estos efectos deben evitarse malas prácticas como dejar los documentos encima de la mesa; dejar las llaves accesibles como, por ejemplo, puestas en la cerradura o en el vaso de los bolígrafos.

Implementación

Deberán habilitarse archivadores y mobiliario de oficina con puertas con llave.

Implicaciones

La guarda y custodia de la documentación bajo llave permite garantizar la confidencialidad, la integridad y la disponibilidad de los datos así como controlar la existencia de incidentes físicos.

mp.sp.2 Destrucción de documentación adecuada

Motivación

Esta medida resulta de aplicación para todos los documentos que contengan datos personales.

Ámbito

La documentación en soporte papel que contenga datos personales debe destruirse bien mediante un servicio de destrucción certificada o bien mediante la utilización de destructoras de papel.
En cuanto a la destrucción certificada de papel, el servicio se solicita llamando a la extensión 6200.
Sobre cómo elegir una destructora:
https://docs.google.com/document/d/1nrYVeC79BU9WDteKpythaqfdEgQQaRGTh9NIDhitaVs/edit?usp=sharing

Implementación

Deberán habilitarse destructoras de papel en los servicios o unidades en los que se traten datos personales en papel.

Implicaciones

Una destrucción adecuada permite garantizar la confidencialidad de los datos personales.

mp.sp.3 Impresión de documentos

Motivación

Esta medida resulta de aplicación para todos los documentos que contengan datos personales.

Ámbito

Con ocasión de la impresión de documentos debemos adoptar medidas para que los mismos no estén accesibles por terceras personas una vez impresos.

Implementación

Deberán adoptarse medidas para que los documentos impresos no estén accesibles a terceros hasta que son recogidos de la impresora por su propietario.
Se recomienda la adopción de medidas como la impresión mediante código de usuario en la impresora; la ubicación de las impresoras en lugares de acceso restringido y no de paso general; la destrucción diaria de documentos no recogidos de la impresora.

Implicaciones

Los documentos impresos con datos personales accesibles a terceros suponen un riesgo para la confidencialidad de los datos personales.

Confirmación de lectura y aceptación del contenido del documento

Tras la lectura del presente documento, es obligatorio cumplimentar el siguiente formulario, para que conste la recepción y lectura del mismo por el usuario de los servicios de la Universidad Carlos III de Madrid

Formulario de confirmación de lectura