UNIVERSIDAD DE GRANADA

PROTOCOLO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD DE DATOS PERSONALES DE LA UNIVERSIDAD DE GRANADA

Tabla de contenido

Primero. Objeto y ámbito de aplicación

1. El procedimiento recogido en el presente documento pretende dar cumplimiento al Reglamento UE/2016/679, Reglamento General de Protección de Datos europeo (RGPD) en materia de detección y notificación de brechas que puedan afectar a la seguridad de los datos de carácter personal incorporados en tratamientos de responsabilidad de la Universidad de Granada, independientemente del formato o soporte en el que estén almacenados u organizados.

2. Asimismo tiene por objeto dar cumplimiento a las obligaciones relativas a la gestión, respuesta y documentación-registro a nivel interno de incidentes de seguridad y hacer notar que, una vez detectada la brecha de seguridad, en función de su naturaleza y alcance, la Universidad de Granada dispone de un plazo de 72 horas para su comunicación a la Autoridad de Control competente, valorar su posible comunicación al Centro Criptológico Nacional (CCN) y, en su caso, cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, su comunicación a los afectados.

3. El presente procedimiento será de aplicación a cualquier usuario de los sistemas de información de la Universidad de Granada implicados en el tratamiento de datos de carácter personal, ya sea miembro del Personal Docente e Investigador (PDI), Personal de Administración y Servicios (PAS), estudiantes o personas externas que se conectan o interactúan con tales sistemas de información vía web institucional o acceso físico a la documentación.

Segundo. Brechas de seguridad. Concepto e identificación

1. Una brecha es una exposición innecesaria de información o datos de carácter personal que puede conducir a su visualización, captura o manipulación por terceros no autorizados.

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" como "todas aquellas violaciones de la seguridad que ocasionen 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." Suelen clasificarse en las siguientes categorías:

- Brecha de confidencialidad: acceso a la información por quien no está

autorizado o tiene un propósito ilegítimo para acceder a ella.

- Brecha de integridad: alteración de la información original y la sustitución de datos puede ser perjudicial para el individuo.
- Brecha de disponibilidad: impide el acceso a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

2. Identificación. Los casos más comunes de posible violación de datos personales son:

• Acceso a datos no autorizados:

- Encargo del tratamiento sin el contrato correspondiente.
- Acceso indiscriminado a impresoras, fotocopiadoras, etc.
- Acceso a información confidencial no autorizada: nóminas, currículos, embargos, videovigilancia, etc.
- Acceso no autorizado a los sistemas informáticos.

• Comunicación no autorizada de datos:

- Transmisión ilícita de datos a un destinatario. Error en la dirección de correo.
- Vulneración del secreto profesional.
- Publicación de imágenes sin autorización del interesado.
- Envío de correos electrónicos masivos sin ocultar los destinatarios (copia oculta).
- Transferencia internacional de datos sin estar sujeta a una decisión de adecuación de la UE o garantías adecuadas de protección de datos.

• Alteración de datos:

- Modificación de datos malintencionada.
- Falsificación de datos.
- Recuperación ineficaz de copias de respaldo.

• Pérdida de información:

- Extravío u olvido de soportes (portátil, "pendrive" o disco externo)
- Robo o sustracción de información (portátil, "pendrive" o disco externo)
- Desinstalación de aplicaciones informáticas.
- Por causas del transporte.
- Reorganización de la empresa.

• Destrucción de datos:

A. No usar destructora de papel o de soportes digitales.
B. Incendio, inundación u otras causas ajenas a la empresa.

• En cualquiera de los casos mencionados anteriormente, se pueden producir violaciones de datos por la ausencia de medidas de seguridad:

- Antivirus, *antispam*, *antimalware*, *antiransomware*, *firewall*, cifrado, "seudonimización", etc.
- Identificación y autentificación para acceder a los sistemas informáticos.
- Mecanismos de seguridad para acceder al mobiliario o a departamentos con datos personales.
- Disposición de datos a la vista de personas no autorizadas (recepción, monitores, mesas, etc.).

Tercero. Plan de actuación.

1. Detectada e identificada una brecha de seguridad por cualquier usuario de los sistemas de información de la Universidad de Granada es necesario comunicarlo internamente a efectos de su análisis, clasificación, elaboración de un plan de respuesta con el diseño de las medidas a adoptar para contener, reducir o eliminar posibles daños y, en su caso inicio del proceso de notificación.

A tal efecto, ante cualquier detección de exposición de datos personales bien sean en lugares que incluyan soportes físicos o informáticos, el usuario deberá cumplimentar el formulario del Anexo II, dando el mayor número de detalles necesarios para su análisis y valoración, y enviarlo, mediante correo electrónico, a la Oficina de Protección de Datos de la Universidad de Granada (protecciondedatos@ugr.es) y al Área de Seguridad Informática del CSIRC (seguridadinformática@ugr.es), sin perjuicio de que, por determinadas circunstancias o por motivos de urgencia, se pueda comunicar telefónicamente al número telefónico 36000 / 958241010 (CAU-CSIRC) o 958240874 (Oficina de Protección de Datos).

2. El Responsable de Área de Seguridad Informática del CSIRC, conjuntamente con el Responsable de la Oficina de Protección de Datos y el asesoramiento del titular de la Delegación de Protección de Datos, analizarán la comunicación para determinar si se está ante una brecha de seguridad relacionada con la protección de datos de carácter personal.

En caso de que lo sea, la Oficina de Protección de Datos o el Área de Seguridad Informática determinarán las medidas correctoras a aplicar y los controles a implementar, comunicándolas a los responsables internos de los tratamientos afectados.

El Área de Seguridad Informática del CSIRC recabará los datos necesarios para, en su caso, comunicarlo a la Agencia de Protección de Datos en el plazo máximo de 72 horas desde su detección y, si procede, a los interesados afectados.

Cuarto. Inscripción de incidentes en el Registro de Brechas de Seguridad de Datos Personales de la Universidad de Granada

1. Ante cualquier incidente, el Área de Seguridad Informática del CSIRC abrirá expediente de seguridad de la información en la aplicación creada para gestionar los "ciberincidentes" anotándolo como "exposición de información", asimismo dará de alta el expediente en el Registro de Brechas de Seguridad de Datos Personales.

2. El Registro de Brechas de Seguridad de Datos Personales, custodiado por Responsable del Área de Seguridad del CSIRC, contará con la siguiente información respecto de cada incidente de seguridad de datos de carácter personal:

A. Tipo de Notificación (N.º registro, fecha y tipo).
B. Datos Delegado de Protección de Datos.
C. Datos del Responsable del Tratamiento.
D. Datos del Encargado del Tratamiento (si lo hubiese).
E. Información temporal de la brecha (fecha de detección, medios de detección, justificación de notificación tardía, fecha de inicio de la brecha, estado de resolución)
F. Sobre la brecha:
    a. Resumen del incidente.
    b. Tipología (confidencialidad, integridad o disponibilidad).
    c. Medio por el que se materializó la brecha.
    d. Contexto.
    e. Medidas preventivas aplicadas antes de la brecha.
G. Sobre los datos afectados:
    a. Categoría de los datos.
    b. Categorías especiales de datos.
    c. Número aproximado de registros de datos afectados.
G. Sobre los sujetos afectados (perfil y número de personas afectadas).
H. Posibles consecuencias:
    a. En brecha de confidencialidad.

   b. En brecha de integridad.
   c. En brecha de disponibilidad.
   d. Naturaleza del impacto potencial sobre los sujetos.
   e. Severidad de las consecuencias para los individuos.
   f. Medidas tomadas para solucionar la brecha y minimizar el impacto con los afectados.

I. Comunicación a los interesados (si se comunica: fecha, número de sujetos informados, medio utilizado, justificación para no informar).
J. Implicaciones Transfronterizas.
K. Datos relativos a incidencia interna (número, fecha, denunciante)

3. El Responsable del Área de Seguridad Informática del CSIRC trasladará mensualmente información de las incidencias registradas a la persona titular de la Secretaría General como Responsable de la Información en la Universidad de Granada, al que corresponde velar por el buen uso de la información y por su protección, e informará, con carácter anual, al Comité de Seguridad previsto en la Resolución del Rectorado de la Universidad de Granada, de 18 de septiembre de 2013, por la que se aprueba la Política de Seguridad de la Información de la Universidad de Granada, modificada por Resolución de 20 de marzo de 2017 y sucesivas modificaciones.

Quinto. Organización de la gestión y comunicación de brechas de seguridad de datos personales

- Responsable de la Información: persona titular de la Secretaría General de la UGR o persona en quien delegue.
- Responsable del Área de Seguridad Informática del CSIRC: análisis y en su caso comunicación de la brecha, así como apertura, si se cree conveniente, de expediente con el CCN (Centro Criptológico Nacional).
- Responsable de la Oficina de Protección de Datos: dará apoyo a la comunicación de la brecha.
- Coordinador de Protección de Datos.
- Titular de la Delegación de Protección de Datos: supervisión/asesoría/mediador en el procedimiento de comunicación.

ANEXO I

Marco legal

Europeo:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (artículos 33 y 34).

Nacional

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (art. 73).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Sectorial

- Política de Seguridad de la Información de la Universidad de Granada. Resolución del Rectorado de la Universidad de Granada, de 18 de septiembre de 2013, por la que se aprueba la Política de Seguridad de la Información de la Universidad de Granada, modificada por Resolución de 20 de marzo de 2017 (Boletín Oficial de la Universidad de Granada, n.º 117, de 27 de marzo de 2017) y sucesivas modificaciones.

UNIVERSIDAD DE GRANADA

ANEXO II

FORMULARIO PARA NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Denunciante o notificante.-

DNI:	Nombre y apellidos:
Teléfono de contacto:	Email:
Unidad/Servicio/Dpto:	

Información temporal de la brecha.-

Fecha de detección de la brecha: _____

Medios de detección de la brecha:

_____

_____

Resumen del incidente.-

_____

_____

☐ Brecha de confidencialidad (acceso no autorizado)
☐ Brecha de integridad (modificación no autorizada)
☐ Brecha de disponibilidad (desaparición o pérdida)

Medio por el que se ha materializado la brecha.-

☐ Datos personales residuales en dispositivos obsoletos
☐ Hacking
☐ Correo perdido o abierto a vista de terceros.
☐ Datos personales mostrados al individuo incorrecto.
☐ Documentación perdida, robada o depositada en localización insegura.
☐ Malware (e.j. Ransomware, virus)
☐ Dispositivo perdido o robado (ordenador, pendrive, disco externo)
☐ Datos personales enviados por error
☐ Eliminación incorrecta de datos personales en formato papel.
☐ Phishing (correo con URL maliciosas)
☐ Publicación no intencionada
☐ Revelación verbal no autorizada de datos personales.
☐ Otros: _____

Medidas preventivas aplicadas antes de la brecha:

_____

_____

Sobre los datos afectados.-

Categoría de los datos afectados:

☐ Datos básicos ☐ Credenciales de acceso o identificación ☐ Datos de contacto

☐ DNI, NIE y/o Pasaporte ☐ Datos económicos o financieros ☐ Datos de localización

☐ Sobre condenas e infracciones penales ☐ Otros:_____

Categorías especiales de datos:

☐ Sobre religión o creencia ☐ Sobre el origen racial ☐ Sobre la opinión política

☐ De salud ☐ Sobre afiliación sindical ☐ Sobre la vida sexual

☐ Desconocidos ☐ Genéticos ☐ Biométricos

☐ Otros:

_____

Número aproximado de registros de datos personales afectados: _____

Sobre los sujetos afectados.-

Perfil de los sujetos afectados:

☐ Estudiantes	☐ Empleados	☐ Usuarios	☐ Proveedores
☐ Otros: _____			

Número aproximado de personas afectadas: _____

Granada a __ de _____ de 2.0__

Fdo:

Información básica sobre protección de sus datos personales aportados	
Responsable:	UNIVERSIDAD DE GRANADA
Legitimación:	El tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento (art. 6.1.c Reglamento general de Protección de Datos).
Finalidad:	Gestionar el trámite de detección, control y respuesta de brechas de seguridad en la Universidad de Granada, procediendo, en su caso, a su notificación a la Autoridad de Control y a los interesados.
Destinatarios:	Autoridad de Control competente
Derechos:	Tiene derecho a solicitar el acceso, oposición, rectificación, supresión o limitación del tratamiento de sus datos, tal y como se explica en la información adicional.
Información adicional:	Puede consultar la información adicional y detallada sobre protección de datos en el siguiente enlace : http://secretariageneral.ugr.es/pages/proteccion_datos/clausulas-informativas-sobre-proteccion-de-datos

ANEXO III

GLOSARIO

***Antimalware*:** programa para evitar cualquier tipo de software malicioso en el ordenador.

***AntiRansomware*:** programa para evitar el cifrado del disco duro mediante un software malicioso, pidiendo posteriormente un rescate por la clave de descifrado.

***AntiSpam*:** *software* para evitar la recepción de correo no deseado.

Antivirus: programa cuyo objetivo es detectar o eliminar virus informáticos.

Autoridad de control: organismo público e independiente que tiene como objetivo principal supervisar la aplicación del RGPD para garantizar la protección de los derechos y libertades de las personas físicas y sancionar su incumplimiento, así como facilitar la libre circulación de los datos de carácter personal en la Unión Europea.

Cifrado: es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.

Dato personal: toda información sobre una persona física identificada o identificable («el interesado»), cuya identidad pueda determinarse, directa o indirectamente; en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Firewall: programa para evitar el control de conexiones desde internet al nuestro ordenador.

***Hacking*:** actividad que realiza un "hacker". Un "hacker" es comúnmente un experto informático que utiliza sus conocimientos técnicos para superar un problema,

normalmente asociado a la seguridad TIC. Habitualmente se lo utiliza en informáticos con conocimientos en seguridad TIC y con la capacidad de detectar errores o fallos en sistemas informáticos para luego informar de los fallos a los desarrolladores del *software* encontrado vulnerable o a todo el público.

Phishing*: *viene del inglés "pescar". Es una técnica de ingeniería social orientada a engañar y hacerse pasar por otra persona para conseguir alguna información. Normalmente se utilizan correos electrónicos engañosos para conseguir claves.

"Seudonimización": es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos. Un pseudónimo único por cada campo reemplazado, o grupo de campos reemplazados, hace cada récord de datos menos identificable mientras se queda apto para análisis de datos y procesamiento de datos.

Tratamiento de datos personales: cualquier operación que se realice sobre datos personales con independencia de que estos sean automatizados o no automatizados, tales como, recogida, acceso, conservación, consulta, comunicación, grabación, bloqueo, supresión.