REGISTRO DE INCIDENTES DE SEGURIDAD SOBRE PROTECCIÓN DE DATOS

IDENTIFICACIÓN DE LA ENTIDAD A LA QUE SE NOTIFICA EL INCIDENTE

- UNIVERSIDAD DE LEÓN (en adelante la ULE)
- CIF: Q2432001B
- Dirección postal: Av. Facultad, 25. 24004 León (España)
- Correo electrónico de contacto: secgen@unileon.es
- Dirección electrónica del Delegado de protección de datos: dpd@unileon.es

Protocolo de actuación ante un incidente de seguridad

Ante la detección de una incidencia de seguridad en la que se hayan visto afectados datos de carácter personal. Bien el propio interesado, por haber sido el que ha podido verse afectado por ese incidente, o cualquier usuario que haya sido conocedor de dicho incidente, sin necesidad de ser el propio afectado, deberá notificar dicho incidente, a la mayor brevedad posible, a la siguiente figura:

1. *Responsable del tratamiento de datos o delegado de protección de datos*: Se aconseja, a la mayor brevedad posible comunicarse con la ULE a través del correo del DPD. También comunicar al correo general de Secretaría General de la ULE el cual está identificado en las líneas anteriores.

Para poder hacer más rápida la comunicación y notificación de la incidencia, se pone a disposición de los usuarios una tabla de recogida de datos relacionados con el incidente de seguridad de la que ha sido víctima, o del que ha tenido constancia.

Recuerde, que cuando hablamos de incidentes de seguridad, no siempre son aquellos sucesos que puedan ocurrir de forma online, sino también offline. Los incidentes de seguridad sobre protección de datos pueden ocurrir de forma física con accesos no autorizados a documentación personal, robos de documentación, perdida de expedientes, exámenes, facturas, etc.

Recogida de datos en relación a incidentes de seguridad en la ULE e información de protección de datos.

Descripción del contesto en el que se ha producido el incidente de seguridad	*Se debe describir todos los aspectos relacionados con el incidente de seguridad. Incluir que se hacía en ese momento, que motivo dicho incidente, si fue causado por un acto ilícito como correo phishing, acceso no autorizado por parte de terceros, perdida de documentación, destrucción accidental, etc)*
Medio por el que se ha materializado la brecha	*(Si ha sido por correo electrónico, robo de documentación física o digital, etc.)*
Categorías de datos afectados	*Describir tipo de datos afectados, nombres, apellidos, DNI, datos bancarios, expedientes, notas, etc)*

Volumen aproximado de registros e interesados afectados	*(Indicar el número aproximado de datos que han sido afectado en el incidente)*
Colectivos afectados	*(Que colectivos están afectado, por ejemplo, alumnos, trabajadores, proveedores, colaboradores, etc)*
Fechas de producción de la brecha de seguridad	*Momento exacto en el que se detecta la brecha*

Tras cumplimentar con este cuestionario de información, se solicitará además los datos del usuario que notifica el incidente de seguridad para que la ULE pueda ponerse en contacto para recopilar más información, en el caso de que fuera necesario para valorar la gravedad o no de la incidencia, o en el caso de que fuera necesaria su colaboración para poder esclarecer los hechos que motivaron dicho incidente.

Nombre/apellidos y correo electrónico y/o número de teléfono de contacto	*Se debe añadir los datos de contacto de la persona que va a notificar la incidencia, para que se pueda poner en contacto la ULE una vez recibida la notificación, y poder recabar más información o datos, si fuera necesario, para tratar dicha incidencia de seguridad, a la mayor brevedad posible.*

Para ello, se incluye esta casilla para que se puedan incluir sus datos de carácter personal, los cuales serán tratados por la UNIVERSIDAD DE LEÓN, con la finalidad de gestionar el potencial problema, incidencia o brecha de seguridad que el usuario va a notificar, y poder comunicarse con él, siempre con relación a cumplir diligentemente con la resolución de cualquier problema. La base de legitimación para el tratamiento de estos datos será el consentimiento previo por parte del interesado al mostrar una clara acción afirmativa por ponerse en contacto con nosotros y notificar la incidencia y sus datos para contacto. Sus datos serán conservados únicamente para la gestión de estas incidencias, tras lo cual serán eliminados o en su defecto bloqueados para depurar posibles obligaciones legales surgidas del tratamiento. No serán cedidos sus datos a terceros. Podrá usted ejercer sus derechos de acceso, rectificación, supresión, portabilidad, limitación y oposición siempre ante el correo dpd@unileon.es, o su defecto ante la Agencia Española de Protección de datos.

FORMULARIO COMPLETO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD EN LA ULE

Este formulario de información se deberá registrar a través de cau.unileon.es en

Informática y comunicaciones → Aplicaciones para usuarios → Seguridad en la red corporativa

Descripción del contesto en el que se ha producido el incidente de seguridad	
Medio por el que se ha materializado la brecha	
Categorías de datos afectados	
Volumen aproximado de registros e interesados afectados	
Colectivos afectados	
Fechas de producción de la brecha de seguridad	
Otros datos relevantes	
Nombre/apellidos y correo electrónico y/o número de teléfono de contacto	