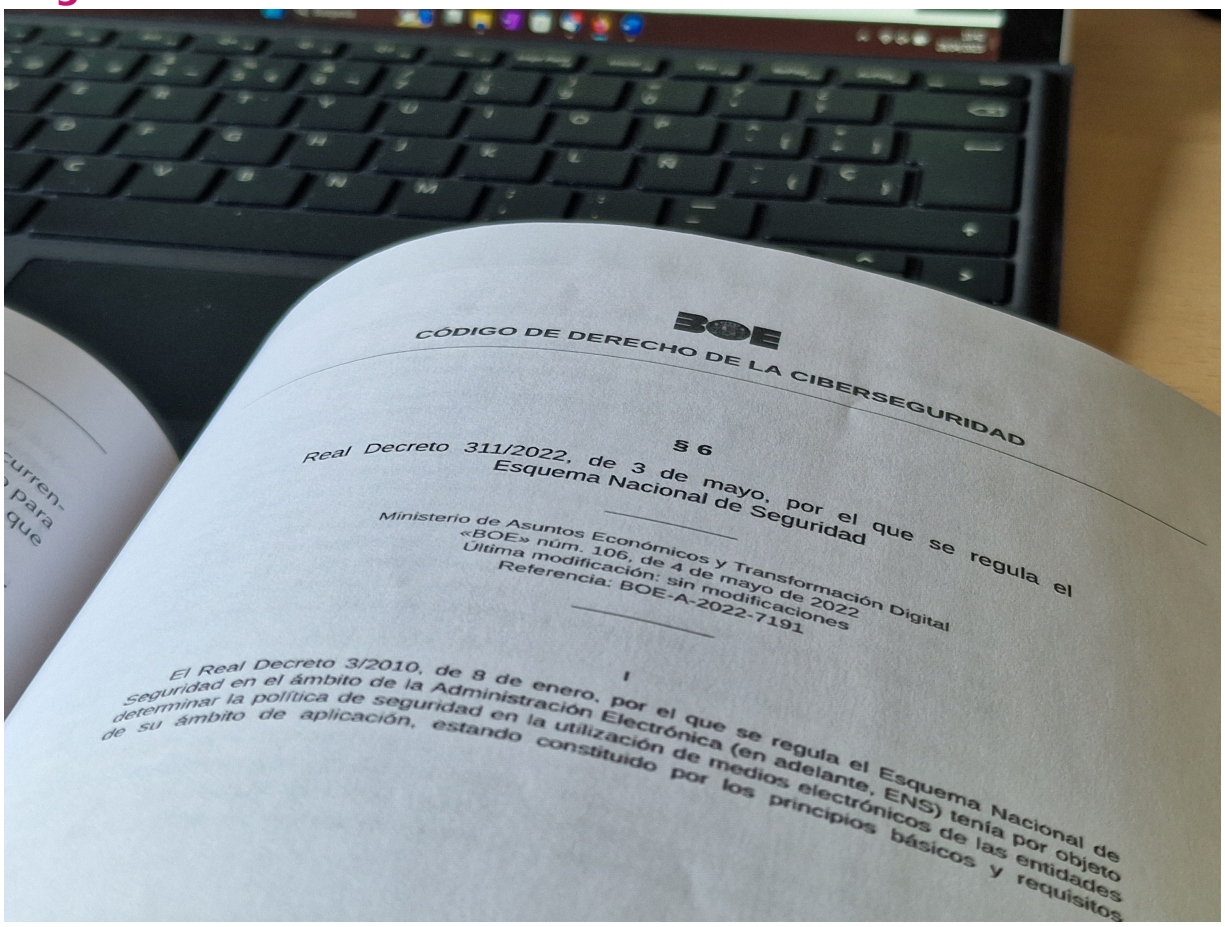
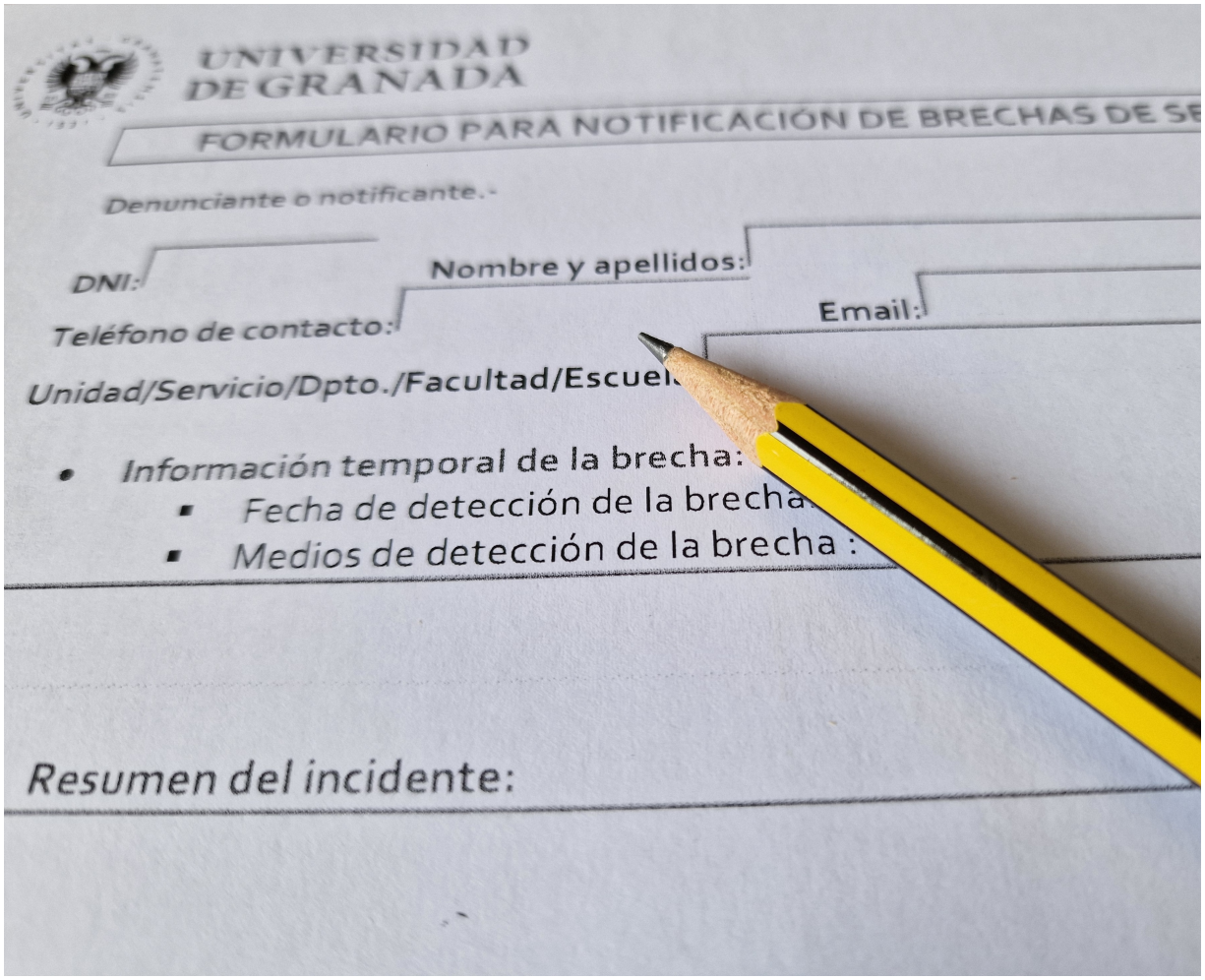
UNIVERSIDAD DE GRANADA

Secretaría General

Seguridad de la Información



Normativa



Reportar Incidente

Decálogo de ciberseguridad

Enlaces

Responsable de la Información

El responsable de la información de la Universidad de Granada es la Secretaria General cuyos datos de contacto son:

- Dirección postal: Hospital real, Cuesta del Hospicio s/n. 18071 Granada
- Correo electrónico: secretariageneral@ugr.es

Responsable de los Servicios

El responsable de los servicios de la Universidad de Granada es el Gerente cuyos datos de contacto son:

- Dirección postal: Hospital real, Cuesta del Hospicio s/n. 18071 Granada
- Correo electrónico: mguardia@ugr.es

Responsable de Seguridad de la Información

La Universidad de Granada ha nombrado como Responsable de Seguridad de la Información a José Antonio Gómez Hernández, que actúa como Secretario del Comité de Seguridad, y al que puede dirigirse para cualquier consulta relativa a la seguridad

de la información a través de los siguientes datos de contacto:

- Dirección postal: Hospital real, Cuesta del Hospicio s/n. 18071 Granada
- Correo electrónico: responsablesi@ugr.es
- Teléfono: 958 240 572

Responsable del Sistema y Administradores de la Seguridad

La responsabilidad del sistema recae sobre el Director del Centro de Servicios de Informáticos y Redes de Comunicación, y la administración de la seguridad sobre las/los jefes de servicio del CSIRC relacionados con la materia.

Finalidad

La Universidad de Granada establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la universidad se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazadas en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de datos personales, con especial atención a las categorías especiales de datos, para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y, en su caso, en materia de protección de datos personales.