Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València (ACGUV 245/2023)

Comentarios a las normas establecidas en el Reglamento

Índice

1. Introducción al Reglamento
2. Normas de seguridad
   - Controles de acceso físico y lógico
   - Uso, mantenimiento y destrucción de dispositivos o soportes que contengan información protegida
   - Salidas y entradas de datos
   - Correo electrónico y red corporativa
   - Recursos informáticos
   - Incidencias de seguridad
   - Información institucional y datos personales
   - Publicación en web

1. Introducción al Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València

El **Esquema Nacional de Seguridad** (Real Decreto 311/2022, de 3 de mayo) establece que las Administraciones públicas dispondrán de un reglamento de seguridad de la información.

La Universitat de València se adaptó en 2014 a los requisitos del Esquema Nacional de Seguridad (ENS) y aprobó su reglamento que fue actualizado en 2021 y 2023.

- **Reglamento de seguridad de la información en la utilización de medios electrónicos** (ACGUV 245/2023).

Objetivos del Reglamento

- **Garantizar** a las personas usuarias **el acceso a la información** con la cantidad y calidad que se requiere para el desempeño de sus funciones.
- **Evitar pérdidas de información** y accesos no autorizados a esta.

El Reglamento es un instrumento **al servicio de la Universitat y de los usuarios y usuarias** capaz de:

- proporcionar **confianza** en los sistemas;
- preservar el **ejercicio de las funciones** y responsabilidades propias de cada persona usuaria;
- garantizar la **calidad y veracidad** de la información objeto de tratamiento.

A quién afecta el Reglamento

- **Personal público** de la Universitat de València.
- **Miembros de comisiones** u órganos relacionados con la Universitat de València.
- **Prestadores de servicios**, entidades colaboradoras o cualquier otro agente con algún tipo de vinculación con la Universitat de València.

Normas de seguridad

- Se define un conjunto de **39 normas sobre 8 aspectos** (situaciones) diferentes.
- Las normas pretenden establecer unas **buenas prácticas** en nuestro trabajo diario, que se pueden extender a otros sistemas de información, aunque no sean los incluidos en el Esquema Nacional de Seguridad (ENS).

Reglamento de seguridad de la información en la utilización de medios electrónicos de la Universitat de València (ACGUV 245/2023)

DESCARGAR

2. Normas de seguridad

Aspectos que alcanzan las normas de seguridad.

- Controles de acceso físico y lógico.
- Uso, mantenimiento y destrucción de dispositivos o apoyos que contengan información protegida.
- Salidas y entradas de datos.
- Correo electrónico y red corporativa.
- Recursos informáticos.
- Incidencias de seguridad.
- Información institucional y datos personales.
- Publicación en web.

Resumen

No se tiene que permitir el acceso de personal externo (no autorizado) a las zonas que contengan infraestructuras TIC o documentación con información protegida.

Comentario

Se trata de evitar la manipulación de los equipos y descargas de información mediante:

- instalación de *software* malicioso en los sistemas;
- manipulación de los sistemas de comunicación;
- uso de dispositivos de almacenamiento portátil;
- fotografías de documentos.

Resumen

Se requiere **identificación personal** en el acceso a los sistemas informáticos de la UV.

Comentario

La identificación proporciona confianza al personal de la UV y la ciudadanía.

- El personal sólo es responsable de su actividad.
- La ciudadana y ciudadano tiene que saber quién y cuándo accedió a su información.

Resumen

Hay que tomar medidas en el trabajo cotidiano para **dificultar el acceso a la información** a terceras personas.

Comentario

Se trata de evitar que terceras personas puedan:

- acceder a nuestro ordenador de trabajo usando nuestro usuario personal;
- visualizar o registrar información sobre otras personas usuarias (ciudadanos y ciudadanas) mostrada en el ordenador de trabajo.

Resumen

Se tienen que **proteger las credenciales de identidad** (usuario y contraseña) que permiten acceder a los recursos TIC de la UV.

Comentario

Las credenciales personales nos identifican en los sistemas y, por lo tanto, nos hacen responsables de las acciones realizadas con estas.

- Es muy importante protegerlas, especialmente la contraseña, y no cederlas a terceras personas.
- La protección de la contraseña es responsabilidad del usuario y usuaria. Si sospechas que alguien pudiera conocerla, cámbiala lo antes posible.

Sobre las contraseñas en la UV

- Las contraseñas personales se almacenan encriptadas en los sistemas informáticos de la UV.
- Nadie en la Universitat conoce nuestra contraseña.
- El equipo técnico de la Universitat nunca pedirá que le proporcionemos nuestra contraseña personal.

Precaución

- Si recibes algún mensaje (correo electrónico) pidiendo tu contraseña o que accedas a una página web externa para introducirla, es un engaño.
- No respondas nunca a este tipo de avisos e informa al Servicio de Informática de la UV.

Resumen

Los accesos a las aplicaciones desde ordenadores externos a la UV se tienen que hacer mediante **mecanismos seguros**.

- De la seguridad en la comunicación se encarga el Servicio de Informática de la Universitat de València, habilitando mecanismos de conexión que aseguren la encriptación en la transmisión de los datos (VPN, https).

Comentario

Si almacenamos información de la Universitat en ordenadores externos a la UV, por ejemplo de otras instituciones, tenemos que asegurarnos que estos **ordenadores cumplan también las medidas de seguridad** establecidas en el Reglamento de seguridad.

Resumen

Se tiene que **evitar que el almacenamiento de documentos en papel con datos protegidos** sea accesible a personas ajenas a la UV.

Comentario

- Destruir los documentos impresos una vez que han dejado de ser útiles.
- Imprimir o fotocopiar sólo aquellos documentos estrictamente necesarios y a doble cara. No reutilizar fotocopias erróneas cuando contengan datos personales.
- Si es necesario almacenar documentos en papel, hay que hacerlo en un lugar no accesible por terceros.

Resumen

Medidas que se tienen que tomar para la **destrucción de información generada** en nuestro trabajo diario que no esté en papel.

Comentario

- La información dejada en las salas de reuniones compartidas puede contener datos personales. Por eso, se tiene que borrar o retirar al acabar la reunión.
- Los soportes informáticos (DVD, memoria USB, etc.) tienen que ser borrados o destruidos adecuadamente.

Resumen

Medidas que se tienen que tomar para **evitar el almacenamiento de información en medios no seguros**.

Comentario

- Añadir componentes de almacenamiento o de comunicación en los ordenadores del puesto de trabajo introduce inseguridad sobre el acceso a los datos almacenados o transmitidos a través de ellos.
- Los servicios de almacenamiento en la nube externos a la UV son cómodos pero inseguros, ya que en general los proveedores tienen libre acceso a la información que contienen.
- La UV dispone de servicios de almacenamiento similares que permiten conservar de manera segura la información (disco.uv.es).

Resumen

Se requiere **autorización para la entrada y salida de información** de la cual es depositaria la UV.

Comentario

- Se prohíbe expresamente el uso de soportes de información extraíbles (dispositivos de almacenamiento USB, memorias *flash*, etc.) con datos confidenciales o restringidos de la Universitat de València, sin autorización de la persona responsable de la Unidad de Gestión.
- Para la portabilidad de información, el medio más seguro es siempre el sistema de almacenamiento virtual de la UV, dado que mantiene la información en servidores de la Universitat.

Resumen

Las comunicaciones efectuadas por el personal usuario de la UV con motivo de su trabajo se tienen que hacer **mediante las cuentas de correo oficiales** y la red de comunicaciones de la UV.

Comentario

- Incluir en los mensajes de correo salientes la cláusula relativa a la confidencialidad de los datos y la utilización del contacto de correo electrónico exclusivamente para el fin de este correo.
- Correo UV → Proporciona confianza para la ciudadana y ciudadano y protege la información.

Resumen

Se requiere **autorización para el envío** por medios telemáticos, a terceras personas, de información de la cual es depositaria la UV.

Comentario

- Tendrá que estar autorizada por la persona responsable de la Unidad de Gestión, para la finalidad exclusiva para la cual sea necesaria.
- Cuando la información sea cualificada como confidencial, sólo será admisible el envío mediante un procedimiento que impida accesos no autorizados.

Resumen

Evitar comportamientos en el uso del correo electrónico e Internet que pudieran **comprometer la seguridad de la información**.

Comentario

Determinados correos electrónicos o páginas web pueden descargar *software* malicioso en nuestros ordenadores y generar:

- descargas de información;
- mal funcionamiento de nuestro sistema;
- ataques a otros ordenadores desde el nuestro.

Resumen

Asegurar la **confianza en el ordenador del puesto de trabajo** con que se procesa la información de la Universitat.

Comentario

- Mantener actualizada la seguridad de los sistemas operativos, antivirus y cortafuegos (*firewalls*) del equipo de trabajo mediante actualizaciones automáticas o con la asistencia del Centro de Atención al Usuario del Servicio de Informática.
- La persona usuaria únicamente podrá instalar los programas para los cuales la Universitat de València tenga licencia de uso en el catálogo de *software* https://software.uv.es.

Resumen

Notificar al Servicio de Informática de la UV cualquier incidencia sobre la seguridad de la información de la cual se pudiera tener conocimiento.

Comentario

La información permitirá resolver el problema y controlar los riesgos.

Resumen

La Universitat de València es responsable de la información depositada por toda persona que tenga acceso a ella en virtud de su trabajo y tiene el deber de guardar confidencialidad.

Comentario

- Las usuarias y usuarios tienen que abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) esta información.
- El deber de guardar el secreto se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universitat de València.

Resumen

- En las páginas web de la UV sólo se debe **publicar información** que sea:
- de carácter público ("No clasificada");
- auténtica e íntegra;
- vigente.

Comentario

Hay que tener especial precaución con los datos personales que se publican en las páginas web.

No se debe causar confusión a la ciudadanía y hay que cuidar la fiabilidad y la vigencia de la información publicada. Es muy importante retirar la información cuando haya perdido vigencia, especialmente cuando incluya datos personales con derecho al olvido.

Si tienes alguna duda concreta sobre seguridad o tratamiento de datos, envía un correo electrónico a *enseg@uv.es* o *lopd@uv.es*, respectivamente.

VNIVERSITAT DE VALÈNCIA