VNIVERSITAT DE VALÈNCIA
Fundació General

[SGSI] NORMATIVA DE SEGURIDAD

ÍNDICE

1. OBJETO

El objeto del presente documento es establecer la **normativa de uso seguro de los sistemas de información** en la Fundació General de la Universitat de València (en adelante, la FGUV), dentro del alcance señalado en el Esquema Nacional de Seguridad.

La seguridad siempre ha sido un concepto presente en todos los sistemas de gestión de la información. Su implementación no es sencilla, dado que abarca todos los eslabones de la cadena de gestión de la información y requiere de un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende además de que exista en todos los niveles una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Por tanto, el usuario final necesita ser **concienciado y culturizado en materia de seguridad de la información** y, al mismo tiempo, debe **disponer de unas normas de obligado cumplimiento** respecto al uso de los sistemas informáticos a su alcance, así como soportes o documentos en papel y, con especial relevancia, en cuanto a preservar la confidencialidad de la información de carácter personal que esté siendo tratada en cumplimiento de la legislación vigente.

El presente documento establece las normas de uso de los dispositivos asignados al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como al acceso y tratamiento de datos de carácter personal, en soporte electrónico y en papel.

Es fundamental que todos los empleados de la FGUV que utilizan equipamiento informático, y accedan o traten información de carácter personal para la realización de sus funciones y tareas, sean conocedores de esta norma.

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la FGUV, que resultan de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ALCANCE

Esta normativa de uso de los sistemas de información es de aplicación a todo el ámbito de actuación de la FGUV, y sus contenidos traen causa de las directrices de carácter más general definidas en la normativa vigente y en la Política de Seguridad de la Información de la FGUV.

La presente normativa es de aplicación y de obligado cumplimiento para todos aquellos **Usuarios/as de los sistemas de información** entendiendo por tales a:

- **todo el personal** que, de manera permanente o eventual, realice sus tareas o preste sus servicios en la FGUV.
- personal en prácticas de la FGUV
- el personal de la Universitat de València con acceso a los sistemas de información de la FGUV
- proveedores externos con acceso a los sistemas de la información de información de la FGUV

Y, de forma especial, la presente normativa se dirige al Responsable de Seguridad y a los responsables de los Sistemas de Información.

Legislación y normativa aplicable

Para la redacción de este documento se han seguido las normas indicadas en los siguientes documentos:

- la Guía "CCN-STIC-821 Normas de seguridad en el ENS" y
- el Anexo I de la Guía "CCN-STIC-822" – Procedimientos de seguridad en el ENS".
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
Responsable de la Seguridad	**Elaborar** la normativa de uso de los sistemas de información.
Comité de Seguridad	**Aprobar** la normativa de uso de los sistemas de información.
Usuarios	**Cumplir** con la normativa de uso de los sistemas de información.

4. NORMATIVA INTERNA DE USO DE LOS SISTEMAS DE INFORMACIÓN

4.1 OBLIGACIONES DE LA FGUV

La FGUV proporciona a los/las usuarios/as el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo. Este equipamiento pasará por un proceso de bastionado previo a su entrega, esto es, el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

En los casos en los que el usuario aporte sus propios dispositivos, la FGUV procederá a establecer las medidas de seguridad adecuadas.

4.2 USO DE LOS DISPOSITIVOS INFORMÁTICOS

Respecto de los dispositivos que son propiedad de la FGUV, están destinados a un uso exclusivamente laboral. Sin embargo, la FGUV autoriza la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados al personal de la FGUV.

Los/las usuarios/as deben cumplir las siguientes medidas de seguridad para el uso del equipamiento informático que se les haya proporcionado para las tareas relacionadas con su puesto de trabajo:

Conexión de otros dispositivos	- No está permitido conectar dispositivos que no estén autorizados a la red de la UV. - Tampoco se pueden conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente (por ejemplo, discos duros externos, pendrive...)
Ubicación del dispositivo	- No está permitido variar la ubicación física de los dispositivos asignados a una ubicación concreta sin autorización previa del Responsable del Sistema.
Configuración del dispositivo	- No está permitido alterar la configuración física, configuración de seguridad ni el software de los dispositivos.

Uso de dispositivos y de la red	- Los dispositivos, así como la red de información que la FGUV pone a disposición de los usuarios están destinados a permitir el desempeño de las funciones y tareas profesionales que estos tienen encomendadas.
Uso de la información	- Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otro distinto del servicio al que está destinada. - El Usuario se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la FGUV en ordenador propio, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de Seguridad y se adopten las medidas de seguridad correspondientes. - Asimismo, los datos contenidos en este tipo de soportes deben ser suprimidos una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. - Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático externo, se deberá restringir el acceso y uso de la información que obra en los mismos. - Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

Identificación y autenticación	- Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por la FGUV son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. - Por cuestiones de seguridad no están permitidas prácticas como: 1. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red de la UV. 2. Intentar modificar o acceder al registro de accesos. 3. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros.
Identificación y autenticación - Doble Factor de Autenticación	Con el fin de reforzar la seguridad del acceso a los sistemas, la FGUV implementa un mecanismo de autenticación multifactor (2FA) para las cuentas de usuario de las plataformas Google Workspace y Microsoft 365. Esta medida está alineada con los principios del Esquema Nacional de Seguridad (ENS), en especial con los relativos a la protección frente a accesos no autorizados. - Todos los usuarios con acceso a información tendrán activo y habilitado el 2FA. - Está prohibido desactivar este sistema de verificación sin autorización expresa del área de Seguridad de la Información. - La pérdida del dispositivo configurado para el segundo factor debe ser comunicada inmediatamente al Departamento de informática.. **Aplicación en Microsoft 365** Para las cuentas de Microsoft 365 se utiliza: Microsoft Authenticator, mediante notificación push o códigos temporales.

	Opcionalmente, se permite el uso de código temporal de seguridad enviado por SMS y/o llamadas telefónica. El acceso al portal de Microsoft y a aplicaciones vinculadas requiere obligatoriamente esta segunda verificación. **Aplicación en Google Workspace** En el entorno de Google Workspace, se emplea el doble factor mediante: Notificaciones push a través de la aplicación Google Authenticator. Opcionalmente, se permite el uso de código temporal de seguridad enviado por SMS y usar códigos de seguridad generados en el panel de administración. **Aplicación SAGE50** En el entorno de Sage50, se emplea el doble factor mediante: Notificaciones push a través de la aplicación de autenticación (Recomendable Google Authenticator). Opcionalmente, se permite el uso de código temporal de seguridad enviado por SMS y/o llamadas telefónicas.

La normativa se complementa en la **Política de uso de dispositivos móviles** y en el **Manual de uso de correo corporativo,** que forman parte del **Manual de Protección de datos de la FGUV.**

4.3 USO DE LA RED CORPORATIVA

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los usuarios internos de la FGUV a la Intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Uso de internet	- La utilización de Internet por parte de los Usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña,
Uso del correo electrónico	- Se considera al correo electrónico corporativo como un instrumento básico de trabajo. - El uso del correo electrónico corporativo es exclusivamente laboral. - El acceso al correo se realizará mediante una identificación consistente proporcionada por el proveedor del servicio. - Los envíos masivos de información, así como los correos que se destinen a gran número de usuarios, serán los estrictamente necesarios, para impedir un colapso del sistema de correo y deberán regirse por el procedimiento de creación de listas de distribución establecido en la FGUV que garantiza el cumplimiento de la normativa de protección de datos. - No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. - La normativa completa sobre el uso del correo electrónico puede consultarse en el **Anexo 13-Manual de correo corporativo** que forma parte del Manual de Protección de datos de la FGUV.
Compartición de contenidos	- Se prohíbe el uso de programas de compartición de contenidos **no autorizados**, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

4.4 ACCESO A APLICACIONES Y SERVICIOS CORPORATIVOS

Tanto el equipamiento informático como todos los recursos facilitados al usuario para la realización de las tareas relacionadas con su puesto de trabajo (tales como aplicaciones

informáticas, servidor de datos, etc.) son propiedad de la FGUV, por lo que deberá hacerse un uso diligente de los mismos.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por la FGUV para el uso de aplicaciones y servicios corporativos:

Identificación y autenticación	- Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante *Usuario* y *contraseña*)
	- Los sistemas que lo permitan (AzureAD para acceder a los equipos y GSuite) aplicarán la siguiente política de contraseñas
	  - Longitud mínima: 8 caracteres
	  - Debe incluir mínimo un carácter, una mayúscula y un número
	  - Obligatoriedad de cambio cada 365 días

Custodia de las contraseñas	- La custodia de la contraseña es responsabilidad del Usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona. - Las contraseñas no deben anotarse, deben recordarse.
Renovación de las contraseñas	- En los sistemas que lo permiten, se le pedirá al usuario que cambie la contraseña cada 365 días. Además, los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente y en sistemas que no permiten el cambio automatizado. Esto garantiza el uso privado de las mismas.
Incidencias con las contraseñas	- Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al Responsable de Seguridad, enviando un email a la siguiente dirección de correo: comitedeseguretat.fguv@uv.es según el **Procedimiento de registro y gestión de incidencias.** Esto resulta también de aplicación a la información en papel.

	El procedimiento se complementa con el **Anexo 4** del Manual de Protección de datos de la FGUV.
Soportes informáticos (*pendrives* y discos duros externos USB, CDs, DVDs, disquetes, etc.)	- La salida de soportes fuera de los locales de la FGUV que contengan datos de nivel Alto debe ser expresamente autorizada por el Responsable de la Información (o Responsable del Tratamiento, si tal figura estuviere personalizada). - La entrada de soportes que contengan datos personales deberá quedar registrada de acuerdo con el **Procedimiento de transporte y entrada y salida de soportes en la FGUV**. Asimismo, el soporte deberá ser dado de alta en el inventario de soportes de acuerdo con procedimiento establecido en la FGUV. - No está permitido el uso de unidades externas de almacenamiento de la información para uso privado, tales como: disquetes, pendrives, discos duros externos, CD-R, DVD-R, etc. - En caso de necesitar desechar un soporte que contenga datos personales, se dirigirá una petición en tal sentido al Departamento de Informática y se destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. El Departamento de Informática cuenta con el equipamiento necesario para destruir la información de forma segura e irreversible - Asimismo, el soporte deberá ser dado de baja del correspondiente inventario.

4.5. FICHEROS EN FORMATO NO DIGITAL.

En relación con los ficheros en soporte o documento papel, el usuario deberá observar las siguientes diligencias indicadas anteriormente con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones de la FGUV.

Archivadores o dependencias	- Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contengan soportes o documentos en papel con datos de carácter personal.
Almacenamiento de documentos	- Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de la FGUV. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.
Custodia de documentos	- Cuando los documentos en soporte papel no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso. - Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada de trabajo - Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes. - Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en las mesas de trabajo, mostradores u otro mobiliario.

Traslado	- En los procesos de traslado de documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y de manera que no pueda verse el contenido, sobre todo, si hubiere datos de carácter personal. - En caso de cambiar de dependencia, el proceso de traslado de los documentos en soporte papel se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad aquellos documentos o soportes en papel donde consten datos de carácter personal.
Destrucción	- No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que la información pueda ser legible o fácilmente recuperable. - A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio que disponga la FGUV.

Incidencias	- Comunicar con la mayor diligencia posible al Responsable de Seguridad (enviado un correo electrónico a comitedeseguretat.fguv@uv.es) las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales. - Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel**,** los sucesos siguientes: o Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal. o Uso indebido de las llaves de acceso. o Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal. o Pérdida de soportes o documentos en papel, con datos de carácter personal. o Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

4.6 INCIDENCIAS DE SEGURIDAD

Los usuarios deberán notificar al departamento de informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Fundació General de la Universitat de València o su imagen, deberá informar inmediatamente al departamento de informática por email a informatica.fguv@uv.es que lo registrará debidamente y elevará, en su caso.

Deberá notificarse al departamento de informática cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

4.7 MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

La FGUV, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente puede:

A. Revisar periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
B. Monitorizar los accesos a la información contenida en sus sistemas.
C. Auditará la seguridad de las credenciales y aplicaciones.
D. Monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.

FGUV llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente, previo aviso al usuario. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El departamento de informática, con la colaboración de las restantes unidades de FGUV, velará por el cumplimiento de la presente Normativa General.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

5. PROCESO DISCIPLINARIO

Todos los usuarios de los sistemas de información y de los recursos informáticos de la FGUV están obligados a cumplir lo establecido en la presente Normativa de seguridad.

Cualquier incumplimiento de lo indicado en la presente Normativa, ya sea de forma intencionada o por un comportamiento negligente, puede dar lugar a la suspensión temporal o definitiva del uso de los recursos y servicios asignados al usuario, sin perjuicio de la revisión de los hechos concretos en el ámbito de la normativa disciplinaria y, de manera general, de las responsabilidades a que, en su caso, hubiere lugar en materia administrativa, civil o penal.

Las consecuencias del incumplimiento para el infractor y las medidas aplicables serán adoptadas de conformidad con las normas que regulan la relación laboral y/o de prestación de servicios entre la FGUV y el usuario.

6. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios de los recursos informáticos y/o sistemas de información de la FGUV deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de seguridad que se encontrará disponible en la Intranet de la FGUV.

Los usuarios de los sistemas de información de la FGUV deberán firmar el siguiente compromiso de cumplimiento de la Normativa de seguridad de la FGUV.

Organización:

Trabajador (Nombre y Apellidos):

DNI número: _____

COMPROMISO DE CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA FGUV

Por medio del presente compromiso, el/la Sr./Sra……como usuario/a de recursos informáticos y sistemas de información de la FGUV, declara haber leído y comprendido la presente **Normativa de seguridad**, y aceptar los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, atender a las modificaciones del documento que le hayan sido debidamente comunicadas, comprometiéndose, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20_