Diputació de València | Protecció de Dades i Seguretat de la Informació

CLASIFICACIÓN: **NIVEL "A"**

(Artículo 43.1 Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia)

NORMAS DE SEGURIDAD PARA LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN

CÓDIGO	N/SEG/USU	**APROBACIÓN**	Decreto nº 15873, de 27 de diciembre de 2022, del Presidente de la Diputación de Valencia

CONTROL DOCUMENTAL

ELABORADO POR:	SUPERVISADO POR:	APROBADO POR:
	Eusebio Moya López	Antoni Francesc Gaspar
Departamento de Protección de Datos y Seguridad de la Información	Jefe Departamento de Protección de Datos y Seguridad de la Información	Presidente Diputación de Valencia

HISTÓRICO DEL DOCUMENTO:

Fecha	Edición	Revisión	Cambios Realizados
27/12/2022	01	01	Aprobación inicial de la norma

FICHEROS: NORMATIVA SEGURIDAD ***LOCALIZACIÓN :***

FECHA DE EMISIÓN: Diciembre 2022

INDICE

INTRODUCCIÓN 1

1. CONCEPTOS BÁSICOS. DEFINICIONES 2

2. NORMATIVA INTERNA DE SEGURIDAD PARA LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN 5

N/SEG/USU-001 Seguridad de la información 5

N/SEG/USU-001-1 Valoración de la información y los servicios 6

N/SEG/USU-001-2 Clasificación de la información 7

N/SEG/USU-001-3 Deber de confidencialidad 8

N/SEG/USU-001-4 Acceso y tratamiento de la información 9

N/SEG/USU-001-5 Salida, archivo y almacenamiento de la información 11

N/SEG/USU-001-6 Copias de seguridad 12

N/SEG/USU-001-7 Análisis y gestión de riesgos 13

N/SEG/USU-002 Seguridad de los medios tecnológicos implicados en el tratamiento de la información 14

N/SEG/USU-002-1 Utilización de los medios tecnológicos 15

N/SEG/USU-002-2 Información en espacios o plataformas de Internet 16

N/SEG/USU-002-3 Normas específicas para dispositivos portátiles y móviles 17

N/SEG/USU-002-4 Soportes electrónicos de información 21

N/SEG/USU-002-5 Borrado y destrucción de soportes electrónicos de información 23

N/SEG/USU-002-6 Uso del correo electrónico..... 24

N/SEG/USU-002-7 Uso de Internet 25

N/SEG/USU-002-8 Uso de impresoras, fotocopiadoras, escáneres y faxes..... 27

N/SEG/USU-002-9 Control de accesos a los sistemas de información 28

N/SEG/USU-002-10 Intercambio de ficheros 30

N/SEG/USU-002-11 Modalidad de teletrabajo 31

N/SEG/USU-003 Seguridad de otros activos de los sistemas de información 33

N/SEG/USU-003-1 Seguridad de locales e instalaciones 33

N/SEG/USU-003-2 Seguridad en el entorno de trabajo 34

N/SEG/USU-003-3 Archivadores y recintos dedicados al almacenamiento de información 35

N/SEG/USU-003-4 Información en soportes no automatizados 36

N/SEG/USU-004 Auditorias de Seguridad 37

N/SEG/USU-005 Normas especiales para videovigilancia 39

N/SEG/USU-006 Incidentes de seguridad 42

N/SEG/USU-006-1 Notificación de incidencias 42

N/SEG/USU-006-2 Registro de incidencias 42

N/SEG/USU-007 Usos indebidos de los sistemas de información .. 44

N/SEG/USU-007-1 Uso abusivo del acceso a Internet 44

N/SEG/USU-007-2 Uso abusivo del correo electrónico 45

N/SEG/USU-007-3 Uso abusivo de otros servicios y sistemas 46

N/SEG/USU-008 Monitorización y aplicación de la presente normativa 47

N/SEG/USU-009 Competencias y responsabilidades 49

N/SEG/USU-010 Información, difusión y formación 53

N/SEG/USU-010-1 Información y difusión ……..... 54

N/SEG/USU-010-2 Actividades formativas ……..... 55

N/SEG/USU-011 Incumplimientos 56

INTRODUCCIÓN

El artículo 43.1 del Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, establece que deberá elaborarse un conjunto de reglas y directrices de carácter obligatorio que desarrollen directamente el contenido de la citada Política o que trasladen al orden interno, mediante las correspondientes normas, el cumplimiento de la normativa legal aplicable en la materia.

Dicho precepto recoge expresamente como integrada en su mandato la denominada Normativa de Seguridad, otorgando el artículo 44.1 la competencia para su aprobación al Presidente de la Diputación o Diputado/a en quien éste delegue.

Por Decreto nº 15873, de 27 de diciembre de 2022, el Presidente de la Diputación de Valencia ha aprobado las presentes Normas de Seguridad para los Usuarios de los Sistemas de Información.

En el presente documento consta la normativa interna relacionada con la seguridad de los sistemas de información de la Diputación de Valencia que deben cumplir los usuarios de dichos sistemas de información. En consonancia con el artículo 4 del citado Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, la presente normativa es de aplicación a todos los departamentos y unidades de la Diputación de Valencia, y resultará de obligado cumplimiento para todos los usuarios de los sistemas de información.

1. CONCEPTOS BÁSICOS. DEFINICIONES

A los efectos previstos en esta normativa, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el *Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia*, aprobado por *Acuerdo del Pleno de la Corporación de 26 de abril de 2022*, aprobación definitiva Bop nº 127 de 5 de julio de 2022, y lo recogido en el siguiente glosario:

a) ***Copia de respaldo o de seguridad (backup)**: Copia de la información en un soporte electrónico que posibilite su recuperación.*

b) ***Comité de Seguridad TIC**. Es el órgano que gestiona y coordina la Seguridad de los sistemas de información TIC de la organización. El Comité se crea y regula en el artículo 32 del Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia. Está integrado por los siguientes miembros:*

- ***Presidente**. El Jefe de Servicio de Informática.*
- ***Vice Presidente**. El Secretario General de la Corporación.*
- ***Secretario.** El Responsable de Seguridad de los Sistemas de Información.*
- ***Vocales.** Los diferentes Responsables de Sistemas de Información delegados, Responsables de seguridad delegados y Administradores de seguridad delegados.*
- ***Una persona designada por el Departamento de Protección de Datos y Seguridad de la Información,** que actuará con voz, pero sin voto.*

- ***El Delegado de Protección de Datos de la Corporación,*** *que actuará en funciones de información y asesoramiento en materia de protección de datos, pero no participará en la toma de decisiones.*

c) ***Ficheros temporales:*** *Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.*

d) ***Incidente o incidencia de seguridad:*** *Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información en cualquiera de sus cinco dimensiones.*

e) ***Información****: Cualquier tipo de dato en cualquier formato (digital o no automatizado), que sea tratado por la Diputación de Valencia en el ejercicio de sus competencias.*

f) ***Responsable de la Información****: Es quien tiene la potestad de establecer las características de una información, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales. Serán responsables de la Información el personal directivo – Jefes/as de Servicio, Jefes/as de Oficina, Directores/as, Coordinadores/as, etc.- bajo cuya dirección se encuentre la correspondiente información. (Arts. 27 y 28 Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia.)*

g) ***Responsable de Seguridad de los Sistemas de Información****: Es quien determina las decisiones para satisfacer los requisitos de seguridad de la*

información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre todas estas cuestiones. Será Responsable de Seguridad de los Sistemas de Información en el ámbito de la Diputación de Valencia quien designe el Comité de Seguridad TIC. (Artículo 29 Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia.)

h) ***Responsable del Servicio**: Es quien tiene la potestad de establecer las características de un servicio, a los efectos de determinar los requisitos en materia de seguridad y de protección de datos personales. Serán responsables del Servicio el personal directivo –Jefes/as de Servicio, Directores/as, etc- bajo cuya dirección se encuentre el correspondiente servicio. (Arts. 26 y 28 Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia.)*

2. NORMATIVA INTERNA DE SEGURIDAD PARA LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN

De conformidad con lo dispuesto en el artículo 3 del Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación de Valencia, las presentes normas son de aplicación a todos los sistemas de información TIC, así como a aquellos sistemas de información de cualquier naturaleza que traten datos de carácter personal, que sean de la titularidad de la Diputación de Valencia o cuya gestión o responsabilidad tenga encomendada, como es el caso de la información municipal.

Queda excluida de forma específica de la aplicación de la presente Política la información tratada por los grupos políticos y/o sus miembros, las centrales sindicales y/o miembros representantes de los trabajadores, siempre que dicha información no forme parte de los activos de información titularidad de la Corporación.

Cuando la información consista en datos de carácter personal, además de las presentes disposiciones se aplicarán las específicas para este tipo de información, contenidas en la *Normativa de Protección de Datos de Carácter Personal*, aprobada por Decreto nº 15874, de 27 de diciembre de 2022, del Presidente de la Diputación.

N/SEG/USU-001 SEGURIDAD DE LA INFORMACIÓN

Las normas de seguridad de la información establecidas en la presente normativa tienen carácter de mínimos. La seguridad podrá verse incrementada en aquellos supuestos en que así lo reclame la criticidad de un sistema de

información, por aplicación del principio de "seguridad coordinada y estructurada" establecido en el Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, o por así decidirlo la organización a través del Comité de Seguridad TIC mediante el establecimiento de líneas estratégicas de la seguridad de los sistemas de información.

N/SEG/USU-001-1 VALORACIÓN DE LA INFORMACIÓN Y LOS SERVICIOS

La información tratada en los sistemas de información de la Diputación de Valencia y los servicios a los que se destina se valorarán, a efectos de seguridad, atendiendo a las cinco dimensiones que comprende el objetivo de la seguridad: Disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad.

Los criterios para la valoración serán establecidos por el Comité de Seguridad TIC, tomando como referencia las recomendaciones del Centro Criptológico Nacional, atendiendo a cómo afectaría un incidente de seguridad a la información tratada o el servicio para:

a) Alcanzar sus objetivos
b) Proteger a los activos a su cargo
c) Garantizar la conformidad con el ordenamiento jurídico

Las valoraciones serán realizadas por cada **Responsable de la Información y del Servicio**, respectivamente. No obstante, podrán establecerse valoraciones estandarizadas de referencia por el Comité de Seguridad TIC, así como propuestas de valoración hechas por el Responsable de Seguridad de los

Sistemas de Información a los responsables correspondientes, que podrán confirmarlas si las consideran adecuadas.

N/SEG/USU-001-2 CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información deberá clasificarse, en función de las **exigencias de confidencialidad**, de acuerdo a los siguientes parámetros:

• **Información PÚBLICA**. Puede ser revelada o puesta a disposición del público en general. El acceso público puede venir impuesto o habilitado por normas legales o, simplemente, por así determinarlo los órganos administrativos competentes.

• **Información RESERVADA**. No puede ser revelada a personas ajenas a la Diputación de Valencia. Es información exclusivamente de uso interno de la Corporación.

• **Información RESTRINGIDA**. Está destinada únicamente a las personas que de modo específico se determine, con independencia de que dichas personas sean empleados de la Corporación o terceros.

• **Información CONFIDENCIAL**. Aquella únicamente accesible por un reducido número de personas en atención a la especial relevancia de su contenido, por las graves consecuencias que su revelación a personas más allá del citado círculo restringido podría acarrear para los intereses generales, los de la Corporación o de determinadas organizaciones, entidades o individuos en particular.

La clasificación de la información conforme a las categorías anteriores deberá ser respetuosa con el marco legal general y específico que resulte de aplicación en cada caso.

La clasificación comporta que cualquier información debe hacer mención al nivel al que está adscrita, de forma que cualquiera que pretenda hacer uso de ella conozca previamente los límites de confidencialidad a los que se haya sujeta. La información clasificada como RESTRINGIDA y CONFIDENCIAL deberá indicar qué personas o entidades están autorizadas para acceder a la misma.

Quienes desempeñen el rol de **Responsable de la Información** –artículo 27 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal- deberán establecer los niveles de clasificación de la información que correspondan y determinar quiénes están autorizados para acceder, así como el régimen de divulgación, distribución o puesta en conocimiento o al alcance de terceros.

N/SEG/USU-001-3 DEBER DE CONFIDENCIALIDAD

La información contenida o tratada en los Sistemas de Información de la Diputación de Valencia es responsabilidad de la Corporación, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros no autorizados (externos o internos) dicha información, salvo autorización expresa del **Responsable de la Información** competente, en los términos expuestos en el apartado N/SEG/USU-001-2.

Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a cualquier tipo de información

gestionada por la Diputación de Valencia deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva, con independencia de que su relación con la Corporación haya finalizado, salvo que dicha información hubiera sido clasificada como PÚBLICA.

Cada **Responsable de la Información** o, en su caso, **Responsable del Servicio**, deberá asegurarse de que el deber de confidencialidad y secreto profesional se establezca de forma expresa en todo tipo de relaciones – administrativas, civiles o mercantiles - que impliquen o supongan acceso o tratamiento de la información, incluidos los servicios de simple alojamiento, transporte o soporte técnico, así como las consecuencias que para la Diputación de Valencia y para los infractores puedan derivarse del incumplimiento de dichos deberes.

N/SEG/USU-001-4 ACCESO Y TRATAMIENTO DE LA INFORMACIÓN

Toda la información contenida o tratada en los Sistemas de Información de la Diputación de Valencia o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a la Corporación y a su personal.

Todo acceso a la información deberá estar previamente autorizado por el **Responsable de la Información** correspondiente. En cumplimiento de los **principios de mínimo privilegio y necesidad de conocer**, los privilegios de acceso otorgados a cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones, limitándose de forma que sólo accedan al conocimiento de aquella información requerida para cumplir sus obligaciones.

Deberá existir una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

Cualquier acceso a información sin la citada autorización, o con una autorización que exceda o no se ajuste a lo estrictamente justificado por las actividades profesionales a desarrollar, será considerado como acceso indebido y dará lugar a las correspondientes responsabilidades.

Los usuarios que por razones del desarrollo de su actividad profesional tengan acceso a la información deben estar informados del contenido de la ley y de la normativa interna sobre la materia, de sus obligaciones al respecto y de las consecuencias que para ellos y, en su caso, para la Diputación de Valencia, implica el incumplimiento de las disposiciones legales y de la normativa interna.

Cuando el acceso o tratamiento de la información por parte de terceros se fundamente en la existencia de una prestación de servicios, **el departamento o unidad que sea responsable de la prestación de servicio** a realizar deberá asegurarse del cumplimiento de todas las garantías de seguridad de la información recogidas en la presente normativa. Para ello, deberá formalizar por escrito un documento de carácter vinculante con el proveedor del servicio donde se recojan las garantías citadas, las obligaciones que asume el proveedor y las consecuencias de su posible incumplimiento.

N/SEG/USU-001-5 SALIDA, ARCHIVO Y ALMACENAMIENTO DE LA INFORMACIÓN

La salida de información de la Diputación de Valencia (en cualquier soporte o por cualquier medio de transmisión) deberá ser realizada exclusivamente por el

personal autorizado por el **Responsable de la Información** correspondiente, autorización que contemplará igualmente a la propia información que sale.

Los usuarios se abstendrán de sacar al exterior cualquier información de la Diputación de Valencia en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, móviles, etc.), así como trasmitir la misma (correo electrónico, Internet, plataformas de intercambio de información, etc) sin contar con la autorización citada en el párrafo anterior.

Requerirá de su cifrado, o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte, la información clasificada como CONFIDENCIAL, cualquier otra que así se determine por el Responsable de la Información correspondiente o por el Comité de Seguridad TIC, así como cuando lo determine el resultado del análisis de riesgos sobre el tratamiento de datos de carácter personal. Todo ello sin perjuicio de lo dispuesto en la presente norma para la información tratada en determinados medios.

En el **archivo de la información** se aplicarán los criterios contenidos en la presente normativa, en el resto de normativa interna que pueda existir sobre la materia, como el Reglamento de Desarrollo de la Administración Electrónica de la Diputación de Valencia, así como por lo dispuesto en el Esquema Nacional de Interoperabilidad (RD 4/2010), las normas sobre patrimonio histórico y archivos, y en el resto de normativa administrativa que pudiese ser de aplicación. En cualquier caso, cuando la información consista en datos de carácter personal su archivo se hará de forma que se garantice el ejercicio de los derechos de acceso, rectificación, supresión y oposición a los interesados.

Con carácter general **queda prohibido alojar información de la Diputación de Valencia en sistemas de información externos**, salvo autorización expresa del Comité de Seguridad TIC que, previa petición del **Responsable de la Información** correspondiente, comprobará la inexistencia de trabas legales para ello y verificará que se pueden garantizar los requisitos de seguridad exigibles al tipo de información de que se trate. Deberá elaborarse un procedimiento que contemple los pasos a seguir para la obtención de la autorización del Comité de Seguridad TIC citada.

Los **ficheros temporales** deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática.

N/SEG/USU-001-6 COPIAS DE SEGURIDAD

Las copias de respaldo o de seguridad garantizan la reconstrucción de la información ante incidentes de seguridad en los que pueda verse afectada la integridad o disponibilidad de la misma. Por tanto, mantener copias de seguridad es una cautela esencial de protección de la información.

Corresponde al Servicio de Informática de la Corporación la realización de la copia de seguridad periódica de los datos alojados en los servidores corporativos, conforme a las directrices y procedimientos que establezca el Comité de Seguridad TIC.

Toda la información de la Diputación de Valencia debe guardarse en las unidades de red asignadas, de manera que se garantice su entrada en los procesos de backup sistemáticos de los datos. Los datos generados por los

usuarios en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en la unidad de red compartida que designe el Servicio de Informática.

N/SEG/USU-001-7 ANÁLISIS Y GESTIÓN DE RIESGOS

El análisis de riesgos, entendido como la utilización sistemática de la información disponible para identificar peligros y estimar los riesgos, resulta fundamental para una adecuada gestión de la seguridad de los sistemas de información.

En cumplimiento del artículo 12 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal, todos los sistemas de información deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Los criterios para el análisis y la metodología a aplicar serán establecidos por la normativa de seguridad aplicable al personal técnico de los sistemas de información TIC, siendo dicho análisis la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos en el Esquema Nacional de Seguridad.

Deberá establecerse un procedimiento con las pautas a seguir para llevar a cabo el análisis y la gestión de riesgos de los sistemas de información. Para la armonización de los análisis, el Comité de Seguridad TIC podrá establecer una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

N/SEG/USU-002 SEGURIDAD DE LOS MEDIOS TECNOLÓGICOS IMPLICADOS EN EL TRATAMIENTO DE LA INFORMACIÓN

Todos los medios tecnológicos puestos a disposición de los usuarios: Ordenadores personales y portátiles, aplicaciones, programas, sistemas de impresión y escaneo de documentos, dispositivos móviles, el acceso a la red corporativa y a Internet, son propiedad de la Diputación de Valencia, y son elementos muy importantes en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

En el presente apartado se recogen las normas de uso debido que todos los usuarios deberán observar en la utilización de los medios tecnológicos que la Corporación pone a su disposición.

N/SEG/USU-002-1 UTILIZACIÓN DE LOS MEDIOS TECNOLÓGICOS

La Diputación de Valencia facilita a los usuarios que así lo precisen los citados medios para el desarrollo de su actividad profesional, es decir, para las funciones encomendadas, por lo que **cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido**.

La configuración e instalación de los medios tecnológicos se reserva exclusivamente al personal técnico del Servicio de Informática de la Diputación de Valencia.

No está permitido:

• Alterar la configuración hardware de los equipos ni conectar otros dispositivos a estos a iniciativa del usuario, así como variar su ubicación.

• Alterar la configuración software de los equipos, desinstalar o instalar programas distintos a la configuración establecida por el Servicio de Informática de la Diputación de Valencia.

• La instalación, utilización o conexión a la red corporativa de cualquier medio tecnológico distinto de los admitidos, habilitados y configurados por el Servicio de Informática de la Corporación sin contar con la debida autorización de dicho Servicio.

• Almacenar información privada, de cualquier naturaleza, en los ordenadores personales y en los recursos de almacenamiento compartidos.

N/SEG/USU-002-2 INFORMACIÓN EN ESPACIOS O PLATAFORMAS DE INTERNET

Todos los espacios y plataformas en Internet o tecnologías similares cuya titularidad corresponda a la Corporación, o que se utilicen en nombre de la

Diputación de Valencia, **deberán cumplir los requisitos de seguridad técnica y jurídica** exigidos por la Ley y por la normativa interna.

A fin de asegurar el debido cumplimiento de los citados requisitos de seguridad, se establecerá un procedimiento que contemple la mecánica a seguir por los diferentes departamentos que pretendan hacer uso de dichos entornos, de forma que se garantice la supervisión previa del Responsable de Seguridad de los Sistemas de Información.

Queda prohibido poner en servicio o utilizar en nombre de la Diputación de Valencia cualquiera de los espacios tecnológicos referidos sin que cumplan los requisitos mencionados.

N/SEG/USU-002-3 NORMAS ESPECÍFICAS PARA DISPOSITIVOS PORTÁTILES Y MÓVILES

A los efectos de este apartado se entiende por dispositivo móvil los ordenadores portátiles, las tabletas, teléfonos móviles tradicionales e inteligentes (smartphones), lectores de libros electrónicos (e-readers), llaves electrónicas, USBs, DVD, y similares.

Los dispositivos portátiles y móviles que resulten necesarios para el desempeño de la actividad profesional serán puestos a disposición de los usuarios por la Diputación de Valencia. **Está prohibido utilizar dispositivos portátiles y móviles no proporcionados por la Corporación para almacenar, acceder, transmitir o tratar de cualquier otro modo información**, salvo si se cuenta con la autorización a que se hace referencia más adelante.

Previamente a su entrega o puesta en servicio **los dispositivos deberán ser objeto de una configuración de seguridad por defecto**, que será realizada por el Servicio de Informática conforme a la naturaleza del dispositivo y siguiendo las directrices que se establezcan en la normativa de seguridad dirigida al personal TIC y las que pueda fijar el Comité de Seguridad TIC.

La configuración de seguridad podrá limitar o restringir la conexión directa a redes externas, los canales, puertos y sistemas de comunicaciones de salida de información (WiFi, Bluetooh, USB's, CD, DVD, tarjetas de red, etc.), así como la instalación y ejecución de software (app's, etc) y los servicios que serán accedidos (e-mail, VPN, CRM…).

La Diputación de Valencia tendrá la potestad, en cualquier caso, al igual que para el resto de medios tecnológicos puestos a disposición de su personal, de la monitorización, el borrado remoto de datos o la realización de auditorías de seguridad sobre dichos dispositivos.

Por defecto, y con carácter general, los citados dispositivos se configurarán para mantener cifrados los datos e informaciones que puedan almacenar, así como las transmisiones de información que, en su caso, puedan autorizarse. Podrá excluirse de esta medida aquella información que esté clasificada como PÚBLICA.

En el momento de poner a disposición los dispositivos a los usuarios, estos deberán de haber sido configurados para que incorporen aquellas medidas de seguridad suficientes para asegurar la protección de la información a lo largo de todo el ciclo de vida del dispositivo.

Existirá un **inventario actualizado de los equipos portátiles y móviles** que permita la identificación personalizada de cada dispositivo, saber a quién y cuándo se hace entrega del mismo, las incidencias que le afecten (robo, pérdida, reparación, etc) así como su baja operativa y su destino tras la misma. Dicho inventario será llevado por el Servicio de Informática de la Corporación.

En principio, los dispositivos portátiles y móviles deberán utilizarse únicamente para fines profesionales, no para fines privados. No obstante, podrá ser autorizado un uso para ambos fines cuando se den las siguientes circunstancias:

a) Que la Corporación disponga de productos tecnológicos que permitan segregar ambas áreas de actividad en los dispositivos y garantizar la incomunicabilidad entre ellas, de forma que quede salvaguardado el derecho a la privacidad sin perjuicio del cumplimiento de todas las normas de seguridad establecidas por la Diputación y las potestades de gestión y control que ésta ostenta.

b) Que el usuario, debidamente informado, acepte expresamente estas condiciones de uso.

Sin perjuicio de las directrices establecidas sobre el uso en general de los medios tecnológicos (N/SEG/USU-002-1) serán de aplicación a los dispositivos portátiles y móviles las siguientes:

• Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, el cual deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.

• La pérdida o sustracción de estos dispositivos se deberá poner inmediatamente en conocimiento del Servicio de Informática de la Corporación, para la adopción de las medidas que correspondan y a efectos de baja en el inventario.

• Los usuarios de estos dispositivos deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por el Servicio de Informática, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.

• Cuando se modifiquen las circunstancias profesionales (término de una tarea, cambio de puesto o funciones, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al Servicio de Informática de la Corporación, al objeto de proceder al borrado seguro de la información almacenada y, en su caso, restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

Podrán utilizarse **dispositivos portátiles o móviles no proporcionados por la Diputación de Valencia** para almacenar, acceder, transmitir o tratar de cualquier otro modo información, únicamente cuando concurra alguno de los siguientes supuestos:

a) Se trate de una necesidad profesional **excepcional, específica y por tiempo muy limitado**.

b) Que la información a tratar se haya clasificado como PÚBLICA.

c) Se trate de los supuestos de teletrabajo indicados en la norma 2-002-11, apartado b, de la presente normativa.

La utilización de los dispositivos en estos casos deberá estar expresamente autorizada por el Responsable de la Información correspondiente, el cual lo comunicará al Comité de Seguridad TIC, y además deberán cumplirse, en el supuesto del apartado a), los siguientes requisitos:

- En ningún caso podrá tratarse de información clasificada como CONFIDENCIAL o cuando así lo determine el resultado del análisis de riesgos sobre el tratamiento de datos de carácter personal.
- La autorización contendrá la motivación y el marco temporal de la necesidad.
- El dispositivo deberá proporcionar el entorno de seguridad que resulte exigible, pudiendo ser comprobado por el Servicio de Informática.
- El usuario/propietario estará sometido a las mismas obligaciones de custodia y de conexiones periódicas, así como la aceptación por su parte de las condiciones de uso, que las descritas anteriormente para los usuarios de dispositivos autorizados para fines profesionales y privados.

N/SEG/USU-002-4 SOPORTES ELECTRÓNICOS DE INFORMACIÓN

A los efectos de este apartado se entiende por soportes electrónicos de información los DVDs, CDs, USBs (pendrives), discos duros externos, tarjetas de memoria (SD, UFC, SM, MMS, etc), llaves inteligentes o electrónicas, cintas magnéticas y cualquier otro soporte similar diferente a los dispositivos indicados en el apartado N/SEG/USU-002-3.

Por razones de seguridad los interfaces de los puestos de usuario que conectan dichos soportes estarán deshabilitados. En caso de ser necesario, el **Responsable de la Información** correspondiente solicitará al Servicio de Informática una solución adecuada que atienda dicha necesidad.

Los soportes electrónicos de información que resulten necesarios para el desempeño de la actividad profesional serán puestos a disposición de los usuarios por la Diputación de Valencia. **Está prohibido utilizar soportes electrónicos de información no proporcionados por la Corporación para almacenar información**, salvo si se trata de información clasificada como PÚBLICA y se cuenta con la autorización del Responsable de la Información correspondiente.

Cada departamento será responsable de la determinación del tipo de soporte a utilizar y de su gestión (etiquetado, inventario, registro, distribución, custodia, borrado y destrucción) conforme a las siguientes especificaciones:

a) **Etiquetado**. Todos los soportes de información deberán ser etiquetados mediante un sistema que permita, solo al personal autorizado, identificar el tipo de información que contienen, el nivel de clasificación y de seguridad de la misma.

b) **Inventariado**. Todos los soportes de información serán inventariados, de forma que puedan ser identificados singularmente. El inventario recogerá, como mínimo, los datos del ciclo vital de cada soporte (alta, incidencias, baja).

c) **Registro**. Deberá llevarse un registro actualizado de entrada y salida de soportes de información. El registro reflejará, como mínimo, el tipo de soporte, la fecha y hora, el emisor y el destinatario, el número de soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción y de la entrega, respectivamente, que deberá estar debidamente autorizada.

d) **Custodia**. Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de cada departamento, mediante las actuaciones descritas en el apartado N/SEG/USU-003-3 y garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial en lo referente a temperatura, humedad y otros agresores medioambientales. No obstante, si se produjese la sustracción, pérdida o acceso indebido a los soportes de información deberá ponerse en conocimiento del Responsable de Seguridad de los Sistemas de Información, a través del sistema de notificación de incidencias de seguridad.

e) **Transporte**. En el traslado de soportes de información se adoptarán las pertinentes medidas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte, especialmente cuando la información contenida en el soporte no haya sido objeto de cifrado. Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente. En caso de sustracción, pérdida o acceso indebido a la información durante su transporte deberá ponerse en conocimiento del Responsable de Seguridad de los Sistemas de Información, a través del sistema de notificación de incidencias de seguridad.

N/SEG/USU-002-5 BORRADO Y DESTRUCCIÓN DE SOPORTES ELECTRÓNICOS DE INFORMACIÓN

El Servicio de Informática procederá al borrado seguro y destrucción de los soportes de información, incluidos los dispositivos portátiles y móviles así como cualquier otro sobre el cual se puedan grabar y recuperar datos, que utilicen los diferentes departamentos de la Diputación de Valencia, y podrá también poner a disposición de los usuarios departamentales herramientas de borrado seguro de sus soportes de información. A tales efectos, deberá disponerse de un procedimiento para el borrado seguro y destrucción de soportes de información.

Está prohibido reutilizar y desechar soportes de información sin que previamente hayan sido objeto de la eliminación permanente de la información que pudieran contener, de forma que resulte imposible su recuperación ni siquiera de forma parcial.

N/SEG/USU-002-6 USO DEL CORREO ELECTRÓNICO

El **correo electrónico corporativo** es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la Diputación de Valencia, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

La utilización del correo electrónico como herramienta de trabajo se ajustará a las siguientes normas generales:

• Todos los usuarios que lo precisen para el desempeño de su actividad profesional dispondrán de una cuenta de correo electrónico para el envío y recepción de mensajes internos y externos a la organización.

• Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por el Servicio de Informática de la Diputación de Valencia.

• El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.

• El correo corporativo será la única herramienta de correo electrónico que deberá utilizarse para los asuntos profesionales.

• Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

• El correo corporativo no será utilizado para el intercambio de ficheros salvo en aquellos supuestos en que así se permita, tal como se recoge en la norma N/SEG/USU-002-10.

N/SEG/USU-002-7 USO DE INTERNET

El **acceso corporativo a Internet** es un recurso centralizado que la Diputación de Valencia pone a disposición de los usuarios, como herramienta necesaria

para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

El acceso a Internet deberá ser autorizado por el responsable del departamento o unidad administrativa, siguiendo el procedimiento interno que se determine, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.

Tendrá la consideración de uso profesional de internet el acceso a actividades formativas regladas a las que el personal tenga derecho y/o autorización en el marco de la normativa legal o interna, que requieran de la utilización de dicho recurso y que se lleven a cabo durante el tiempo de trabajo.

Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados por el Servicio de Informática en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo sin la debida autorización del Servicio de Informática.

La utilización de Internet debe obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales tendrá carácter extraordinario, debiéndose limitar su utilización dentro de un tiempo razonable que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

La Diputación de Valencia velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal como desde los riesgos de seguridad asociados a su uso. En este sentido, bajo los criterios

establecidos por el Comité de Seguridad TIC, podrán implementarse herramientas que restrinjan o limiten los accesos a determinados contenidos, categorías de páginas web, ubicaciones o las acciones de los usuarios (descargas, instalación de componentes, ejecución de determinado software, etc). De igual forma, podrán establecerse diferentes niveles de acceso de los usuarios, según la necesidad de utilización de Internet de los mismos.

N/SEG/USU-002-8 USO DE IMPRESORAS, FOTOCOPIADORAS, ESCÁNERES Y FAXES

Con carácter general deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario.

Cuando se imprima, fotocopie, digitalice o se remita por fax documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de los equipos implicados, para evitar que terceras personas puedan acceder a la misma. Conviene no olvidar retirar los originales de la fotocopiadora, impresora, escáner o fax una vez finalizado el proceso correspondiente. Si se encontrase documentación abandonada en una fotocopiadora, impresora, escáner o fax, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del superior jerárquico.

Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde

habrán de almacenarse las imágenes obtenidas, especialmente si contienen información no clasificada como PÚBLICA.

Sin perjuicio de las pautas anteriormente descritas para los usuarios, el Servicio de Informática deberá elaborar rutinas automatizadas para el borrado periódico de la información que pueda quedar almacenada en las carpetas, directorios o memoria de los dispositivos o recursos compartidos para la fotocopia, impresión, escaneado o transmisión por fax.

N/SEG/USU-002-9 CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

Corresponde al Servicio de Informática de la Corporación establecer los diferentes mecanismos que garanticen el acceso a las redes, aplicaciones y datos únicamente a los usuarios y procesos debidamente autorizados. La naturaleza de los citados mecanismos será la que resulte más adecuada en función de los requisitos de seguridad específicos para cada caso, en virtud de las directrices fijadas para ello por el Comité de Seguridad TIC.

Deberá elaborarse un procedimiento que establezca las pautas a seguir para la petición de acceso de usuarios a los sistemas de información, así como para la baja y eliminación efectiva de los derechos de acceso.

Los mecanismos que se pongan a disposición de los usuarios para su debida identificación y autenticación en los sistemas de información podrán consistir en claves concertadas, contraseñas, tarjetas de identificación o cualquier otro dispositivo físico (tokens) o componentes lógicos (certificados software), mecanismos biométricos, o cualesquiera otros de análoga naturaleza.

Dichos mecanismos serán personales e intransferibles, y deberán proporcionar una identificación individual e inequívoca. Los usuarios son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado, por lo que no deberán en ningún caso revelar o entregar, bajo ningún concepto, sus mecanismos de credenciales de acceso a terceras personas, ni siquiera a otros usuarios o personal al servicio de la Diputación de Valencia, ni mantenerlas por escrito a la vista o al alcance de terceros. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar la correspondiente **incidencia de seguridad**. Del mismo modo deberá actuarse cuando se produzca la pérdida o extravío del mecanismo, un mal funcionamiento o cualquier otro comportamiento anómalo del mismo.

Se establecerán las medidas necesarias para limitar el número de intentos de acceso fallidos a los sistemas de información, de forma que, una vez superado éste, se produzca el bloqueo automático del usuario. De igual forma, cuando se utilicen contraseñas deberán incorporarse medidas que fuercen al usuario al cambio periódico de las mismas. El límite de intentos de acceso fallidos, la periodicidad para el cambio de contraseñas y la política de calidad de éstas serán determinados por el Comité de Seguridad TIC.

Deberá elaborarse un procedimiento para la asignación, distribución y almacenamiento, en su caso, de los mecanismos utilizados para la identificación y autenticación en los sistemas de información.

N/SEG/USU-002-10 INTERCAMBIO DE FICHEROS

Únicamente se procederá a la remisión de ficheros mediante las aplicaciones y canales que se determinen por el Servicio de Informática, de forma que quede garantizada la seguridad, confidencialidad y trazabilidad de la información transmitida. Utilidades como el correo electrónico corporativo, entornos FTP y otras en modo nube –drive, icloud, Dropbox, etc- o similar **no se utilizarán para el intercambio de ficheros** salvo que se trate de información clasificada como PÚBLICA o exista una autorización expresa del Servicio de Informática.

Cuando el intercambio de ficheros se produzca con ocasión de la prestación de servicios contratados por la Diputación de Valencia, el Servicio responsable impondrá al proveedor el canal de intercambio según lo indicado en el párrafo anterior. En los instrumentos vinculantes de contratación se hará constar esta circunstancia, debiendo constituir ésta una condición obligatoria de la prestación.

Si el intercambio de ficheros es consecuencia de la asistencia de la Diputación de Valencia a las Entidades Locales se procederá de igual modo. El Servicio responsable de dicha asistencia comunicará esta circunstancia a la Entidad Local receptora de la asistencia, informando de su carácter obligatorio para el desarrollo de la asistencia. Siempre que exista un instrumento administrativo que regule o recoja los términos de la asistencia –convenio, acuerdo, etc- deberá hacerse constar en él dicha circunstancia.

En aquellos supuestos de colaboración administrativa o percepción de prestaciones de otras entidades públicas en los que la Diputación de Valencia no pueda imponer estas condiciones para el intercambio de ficheros, se intentará que dichas entidades acepten el canal propuesto por la Diputación por lo menos

para la remisión de los ficheros por parte de la Diputación, siempre que sea posible.

Las aplicaciones y canales que deban determinarse por el Servicio de Informática para el intercambio de ficheros serán consensuados previamente en el seno del Comité de Seguridad TIC.

N/SEG/USU-002-11 MODALIDAD DE TELETRABAJO

Cuando se lleve a cabo la prestación de servicios en la modalidad de teletrabajo al amparo del Reglamento de prestación de servicios mediante teletrabajo (sector no sanitario), aprobado por acuerdo del Pleno de la Corporación de 23 de noviembre de 2021, se aplicarán las siguientes reglas:

a) En el caso de teletrabajo derivado de necesidades organizativas, así como en aquellos supuestos recogidos en el Capítulo IV del citado Reglamento de Teletrabajo -Otras modalidades de acceso al teletrabajo- en que al personal afectado se le facilite el equipamiento informático y las aplicaciones informáticas por parte de la Diputación, se aplicarán las mismas reglas de seguridad de la información contenidas en las presentes Normas de Seguridad para los Usuarios de los Sistemas de Información, así como las singularidades recogidas en el Reglamento de Teletrabajo, en especial:

   ▪ Que la persona que se acoja a la modalidad de teletrabajo deberá disponer de un sistema de comunicación y conectividad que cumpla con las características técnicas que determine la delegación que tenga atribuidas las competencias en informática y nuevas tecnologías.

▪ Que el equipamiento informático y las aplicaciones informáticas suministradas serán de uso exclusivamente laboral.

▪ Que la persona que preste su servicio mediante teletrabajo será la responsable de custodiar y devolver en las mismas condiciones el equipamiento que le fuera suministrado.

▪ Que corresponderá al empleado o empleada la comunicación de las incidencias que puedan producirse en el equipo informático. En el supuesto de producirse deficiencias o desperfectos derivados de un uso inadecuado o negligente la Diputación podrá exigir las responsabilidades oportunas al empleado o empleada correspondiente.

▪ Que cuando se produzca un mal funcionamiento en el equipo informático o en las aplicaciones instaladas en él, así como en el servidor o plataformas que permitan el teletrabajo, que impidan el trabajo desde la oficina a distancia y que no pueda ser solucionado el mismo día en que ocurrieran o el siguiente, la persona teletrabajadora deberá reincorporarse a su centro de trabajo, reanudando el ejercicio de su actividad en la modalidad de teletrabajo cuando quede resuelto el problema técnico.

b) En los restantes supuestos de teletrabajo distintos a los indicados en el apartado a), en los cuales los dispositivos y/o elementos informáticos utilizados sean por cuenta de la persona teletrabajadora, será de aplicación lo dispuesto para los **dispositivos móviles no proporcionados por la Diputación de Valencia** en la norma N/SEG/USU-002-3 Normas específicas para dispositivos portátiles y

móviles, así como las reglas de seguridad singulares que puedan determinarse por el Servicio de Informática en cada caso concreto.

En todos los supuestos de prestación del servicio mediante la modalidad de teletrabajo, podrán establecerse medidas de seguridad complementarias o distintas a las previstas en la normativa interna de seguridad de la información cuando así lo aconseje el resultado de la evaluación de riesgos. En dichos supuestos, el personal afectado será informado debidamente de las citadas medidas y vendrá obligado a su cumplimiento.

N/SEG/USU-003 SEGURIDAD DE OTROS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN

N/SEG/USU-003-1 SEGURIDAD DE LOCALES E INSTALACIONES

Exclusivamente el personal autorizado podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información. Las condiciones de seguridad que deben reunir dichos recintos serán establecidas en la normativa de seguridad dirigida al personal TIC.

Los locales que se utilicen para la atención al público evitarán ubicar en las zonas accesibles a éste, o en zonas de paso, elementos de los sistemas de información como impresoras, faxes, fotocopiadoras, archivadores, etc.

Siempre que resulte posible los locales se distribuirán de forma que los puestos de trabajo se ubiquen atendiendo a unos mismos o similares privilegios de acceso a la información, así como al uso de recursos compartidos.

N/SEG/USU-003-2 SEGURIDAD EN EL ENTORNO DE TRABAJO

Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Aquella documentación que no se vaya a utilizar en el momento deberá guardarse en cajones bajo llave o en los armarios o archivadores correspondientes.

Cualquier usuario que se ausente temporalmente de su puesto de trabajo deberá bloquear la sesión de su ordenador (salvapantallas con contraseña, etc) para impedir el acceso de otras personas a la información y al equipo informático. Se establecerán bloqueos de sesión automáticos por tiempo de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Al final de la jornada de trabajo los usuarios deberán asegurarse de que el equipo está apagado y que no se deja accesible documentación ni soportes de información de ningún tipo.

Cuando se utilicen pizarras y *flipcharts* los usuarios deberán asegurarse de que se limpian adecuadamente, para que no quede ningún tipo de información a la vista, antes de abandonar las salas o despachos donde se ubiquen o permitir que alguien ajeno entre.

La comida y bebida pueden dañar tanto a los componentes electrónicos como a los soportes de información, por lo que no deberán realizarse estas acciones en el puesto de trabajo, salvo que se adopten todas las garantías que impidan el riesgo de daño mencionado.

N/SEG/USU-003-3 ARCHIVADORES Y RECINTOS DEDICADOS AL ALMACENAMIENTO DE INFORMACIÓN

Los armarios, archivadores u otros elementos en los que se ubiquen los soportes de información deberán disponer de mecanismos de cierre que impidan el acceso a personas no autorizadas.

Siempre que sea posible, dichos armarios o archivadores deben encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los soportes de información que contienen.

Deberá evitarse el almacenamiento, depósito o archivo de soportes de información en recintos o armarios de uso común, salvo que se garantice la existencia de mecanismos que hagan posible el acceso a la información únicamente al personal autorizado en cada caso.

Las dependencias destinadas al archivo de información no se utilizarán para otros usos, como el de almacén de papelería, de utensilios informáticos, material de limpieza, taquillas y vestidores o cualquier otra utilidad que suponga el acceso a dichos recintos de personal distinto al autorizado para acceder a la información almacenada.

Dichas dependencias dispondrán de las debidas garantías medioambientales que impidan cualquier daño o deterioro de los soportes de información, así como

de mecanismos de detección y extinción de incendios adecuados al tipo de soportes que contengan.

N/SEG/USU-003-4 INFORMACIÓN EN SOPORTES NO AUTOMATIZADOS

Toda la información en soportes no automatizados (documentos en papel, carpetas, expedientes, dossieres, etc) deberá ubicarse en armarios, archivadores y recintos con las características que se establecen en el apartado N/SEG/USU-003-3.

Mientras la documentación no se encuentre archivada en los dispositivos de almacenamiento citados, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sin perjuicio de lo que pueda establecer la normativa sobre procedimiento administrativo que en cada caso resulte de aplicación, cuando se trate de documentación que contenga información clasificada como CONFIDENCIAL o cuando lo determine el resultado del análisis de riesgos sobre el tratamiento de datos de carácter personal**,** se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

La generación de copias o la reproducción de los documentos únicamente podrá llevarse a cabo bajo el control del personal autorizado. Las copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares estarán sujetas a los mismos requisitos de

seguridad que los documentos originales, y deberán ser destruidas una vez hayan dejado de ser necesarias para los fines que motivaron su creación.

La destrucción de los documentos que contengan información no clasificada como PÚBLICA, incluyendo las copias o reproducciones, se realizará mediante máquinas destructoras, de forma que se evite la recuperación o reconstrucción de la información con posterioridad.

Siempre que se proceda al traslado físico de documentos que contengan información no clasificada como PÚBLICA, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

N/SEG/USU-004 AUDITORÍAS DE SEGURIDAD

En función de su objeto, se distinguirán dos tipos de auditoria de seguridad:

a) Auditorías comprendidas en el Plan general Auditor de Protección de Datos personales y Seguridad de la Información de la Diputación, que tendrán carácter periódico para evaluar el cumplimiento de la normativa sobre seguridad y la efectividad de las medidas adoptadas. Son las llevadas a cabo por el Departamento de Protección de Datos y Seguridad de la Información, en cumplimiento del artículo 35 del Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia.

b) Auditorías reglamentarias, regulares o extraordinarias, en cumplimiento del Esquema Nacional de Seguridad. El objeto de estas auditorías de la seguridad, internas o externas, es el contenido en el artículo 31 del

Esquema Nacional de Seguridad, el cual determina que los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad; y también que, con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. Son auditorías obligatorias y de carácter reglamentario.

Los informes de resultados de las auditorías periódicas de seguridad que afecten a tratamientos de datos de carácter personal, se gestionarán de acuerdo con las indicaciones del Departamento de Protección de Datos y Seguridad de la Información y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de la Comunidad Autónoma. Además, el Delegado de Protección de Datos deberá de supervisar dichas auditorías, en virtud de lo establecido en el artículo 37 del citado Reglamento.

Los informes de auditoría serán analizados por el Responsable de Seguridad de los Sistemas de Información y por el Departamento de Protección de Datos y Seguridad de la Información, que presentarán sus conclusiones al Comité de Seguridad TIC para que adopte las medidas correctoras adecuadas.
En el caso de los sistemas críticos y de categoría ALTA, visto el dictamen de auditoría, el Responsable de los Sistemas de Información podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

Todos los empleados de la Corporación están obligados a facilitar cuanta información le sea requerida por el personal que lleve a cabo las auditorías

recogidas en el presente apartado, así como el acceso a locales, instalaciones, equipos, archivos, soportes de almacenamiento, programas, procesos y procedimientos.

N/SEG/USU-005 NORMAS ESPECIALES PARA VIDEOVIGILANCIA

Los equipos informáticos utilizados para la captación, almacenamiento y procesamiento de las imágenes y sonidos con fines de videovigilancia deberán tener las siguientes características:

• No serán utilizados para ninguna labor diferente a la de videovigilancia, por lo que el único software que contendrán será el necesario para dicha función.

• Se configurarán de modo que, salvo los mecanismos de transmisión de la información con el centro de proceso de datos, se encuentren inhabilitadas las posibilidades de conexión con redes externas y la entrada-salida de información (WiFi, Bluetooth, USB's, CD, DVD, etc.).

• Preferentemente los equipos locales no almacenarán la información recabada, siendo recomendable que ésta se transmita al centro de proceso de datos remoto. Si las circunstancias técnicas impidiesen o hiciesen muy gravosa dicha transmisión, podrán habilitarse dispositivos de almacenamiento local autónomos (diferentes al disco duro integrado en el equipo local desde el que se gestionan los elementos de captación de las imágenes) siempre que se encuentren ubicados en recintos con control de acceso restringido y dispongan de mecanismos de autenticación para el acceso a la información.

• El acceso o inicio de sesión al sistema estará protegido por un mecanismo de autenticación que identifique a quien accede y solo permita el acceso a usuarios autorizados. El **protocolo de actuación en materia de videovigilancia** descrito en la norma N/PDP-014 contendrá las especificaciones que deberá tener el mecanismo de autenticación.

• Los equipos estarán fuera del alcance del personal no autorizado. Siempre que las características de las instalaciones y del servicio lo permitan, se habilitará un recinto cerrado e independiente para la ubicación de los equipos informáticos locales de videovigilancia que facilite el control de acceso a personas no autorizadas. En caso de no disponer de dicho recinto, los equipos se situarán en lugares bajo el control permanente del personal de vigilancia y se dispondrán de manera que las imágenes no puedan ser visualizadas por terceros.

Para garantizar que el acceso a los sistemas, a los datos y a los soportes que los contengan se limita al personal autorizado que determina la norma N/PDP-014-3, el personal adscrito al servicio de vigilancia de los locales e instalaciones de la Diputación de Valencia será responsable de impedir que el personal no autorizado:

- Acceda físicamente a los recintos donde se ubiquen los equipos informáticos, en caso de que existan recintos con dicha función.
- Acceda a imágenes y/o sonidos recogidos, aunque sea en tiempo real.
- Manipule de cualquier forma los equipos y soportes informáticos.

Se dispondrá de un **centro de control** en el que se almacenarán todas las grabaciones generadas por los sistemas de videovigilancia de la Diputación de Valencia. Dicho centro será el responsable de:

- Mantener las condiciones de seguridad de los datos y de los soportes que los contengan.
- proporcionar a la Diputación de Valencia los datos de que disponga cuando le sea requerido por ésta a través del personal debidamente autorizado.
- Asegurar la transmisión de los datos desde los terminales locales de videovigilancia a los servidores del centro.

Las condiciones específicas de seguridad que debe reunir el centro de control serán establecidas en el **protocolo de actuación en materia de videovigilancia**, atendiendo a la normativa de seguridad de la información de la Corporación y a los riesgos a los que en cada momento se esté expuesto. De igual modo, en el citado protocolo se especificarán los plazos de mantenimiento de la información y el procedimiento para proporcionar datos a requerimiento de la Diputación de Valencia.

N/SEG/USU-006 INCIDENTES DE SEGURIDAD

Deberá elaborarse un procedimiento general que establezca las pautas de actuación de los usuarios de los sistemas de información ante incidentes que puedan afectar a la seguridad de la información. Dicho procedimiento incluirá, en cualquier caso, los cauces para notificar las incidencias y la información requerida.

N/SEG/USU-006-1 NOTIFICACIÓN DE INCIDENCIAS

Es obligación de cualquier usuario comunicar todas aquellas incidencias de seguridad que se produzcan en el ámbito de los sistemas de información. Las incidencias serán reportadas al Responsable de Seguridad de los Sistemas de Información para su correspondiente gestión y posterior información, en su caso, al Comité de Seguridad TIC.

Se habilitará un mecanismo electrónico para la comunicación de incidencias. De igual modo, se implementarán sistemas de detección y notificación automática de incidencias.

N/SEG/USU-006-2 REGISTRO DE INCIDENCIAS

Todas las incidencias que se comuniquen o notifiquen quedarán registradas. Dicho registro se ajustará, como mínimo, a lo siguiente:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

b) Se registrarán aquellas evidencias que puedan, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

En el supuesto de que la incidencia pueda afectar a datos personales, además, en virtud del artículo 33.3 RGPD, en dicho registro deberá constar:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

N/SEG/USU-007 USOS INDEBIDOS DE LOS SISTEMAS DE INFORMACIÓN

Con carácter general, se considerará uso indebido de los sistemas de información en el ámbito de la Diputación de Valencia cualquier conducta contraria a lo dispuesto en la presenta normativa por parte de los obligados a su cumplimiento. No obstante, se enumeran seguidamente un conjunto de acciones que se considerarán específicamente como uso indebido de los sistemas de información de la Diputación de Valencia.

N/SEG/USU-007-1 USO ABUSIVO DEL ACCESO A INTERNET

Será considerado uso abusivo del acceso a Internet:

• El acceso a otras redes con el propósito de violar su integridad o seguridad.

• El acceso a contenidos no relacionados con los cometidos profesionales del usuario excediendo un tiempo razonable, que interfiera en el rendimiento profesional o en la eficiencia de los recursos informáticos corporativos

• Utilizar el acceso a Internet para el uso de mensajería instantánea (WhatsApp, Messenger, Facebook Messenger, Skype, Line, Discord, Google Chat, Telegram, ShazzleChat, etc).

• La transferencia de ficheros no relativa a las actividades profesionales del usuario (tales como juegos, ficheros de sonido, fotos, videos o películas, etc.).

• El acceso a recursos y páginas *web*, o la descarga de programas o contenidos, que vulneren la legislación en materia de Propiedad Intelectual.

• La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.

• El acceso a Internet para realizar cualquier actividad de promoción de intereses personales.

• La publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad

personal y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo ésta o cualquier otra norma interna que pudiera resultar de aplicación.

N/SEG/USU-007-2 USO ABUSIVO DEL CORREO ELECTRÓNICO

Será considerado uso abusivo del correo electrónico corporativo:

• Utilizar el correo electrónico corporativo para fines distintos a los derivados de las actividades profesionales.

• La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a la organización, o el reenvío automático del correo corporativo a buzones ajenos a la organización.

• Usar cualquier cuenta del correo corporativo para enviar mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo ésta o cualquier otra norma interna que pudiera resultar de aplicación.

N/SEG/USU-007-3 USO ABUSIVO DE OTROS SERVICIOS Y SISTEMAS

Será considerado también uso abusivo:

• El acceso a servicios y/o contenidos de los sistemas de información con el propósito de violar su integridad o seguridad.

• La ejecución de programas informáticos en los sistemas de información de la Corporación sin la correspondiente licencia de uso.

• La reproducción, modificación, cesión, transformación o comunicación de los programas informáticos propiedad de la Corporación, salvo que los términos del licenciamiento lo permitan y se cuente con la autorización previa.

• El uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización.

• La transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

N/SEG/USU-008 MONITORIZACIÓN Y APLICACIÓN DE LA PRESENTE NORMATIVA

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

a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

b) Monitorizará los accesos a la información contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y aplicaciones.

d) Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

La Diputación de Valencia llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales 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. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El Responsable de Seguridad de los Sistemas de Información y el Departamento de Protección de Datos y Seguridad de la Información, cada cual en el marco de sus competencias, con la colaboración de las restantes unidades de la Diputación de Valencia, velarán por el cumplimiento de la presente normativa general e informarán al Comité de Seguridad TIC sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

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.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino, conforme a los criterios establecidos para ello por el Comité de Seguridad TIC. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al Responsable de Seguridad de los Sistemas de Información sobre usos prolongados e indebidos del servicio.

Los **registros de actividad** que puedan ser utilizados como prueba en un procedimiento sancionador administrativo o en un proceso judicial gozarán de las garantías tecnológicas que aseguren que no pueden ser alterados. Estos registros **se encontrarán bajo la custodia directa del Responsable de Seguridad de los Sistemas de Información**, que será el único que tenga permisos de acceso a la totalidad de sus contenidos, sin perjuicio de las atribuciones y competencias del Departamento de Protección de Datos y Seguridad de la Información y, en su caso, del Delegado de Protección de Datos.

N/SEG/USU-009 COMPETENCIAS Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Conforme establece el artículo 29 del Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación de Valencia, y sin perjuicio de lo establecido en la norma en relación con las medidas de seguridad de los datos de carácter personal, el **Responsable de Seguridad de los Sistemas de Información** es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reporta sobre estas cuestiones.

En concreto, **al Responsable de Seguridad de los Sistemas de Información le corresponde:**

• Actuar como Secretario del Comité de Seguridad TIC.

• Convocar al Comité de Seguridad TIC, recopilando la información pertinente.

• Ser responsable, junto con los diferentes responsables de seguridad delegados, en su caso, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que puedan afectar directa o indirectamente a la seguridad de los sistemas de información de la Corporación, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad TIC y proponiendo las acciones oportunas de adecuación al nuevo marco normativo.

• Elaborar y firmar las pertinentes Declaraciones de Aplicabilidad de los sistemas de información.

• Ser el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad TIC. Estas decisiones estarán presididas por los principios

de unidad de acción y coordinación de actuaciones en general y, en especial, en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

• En caso de desastre se incorporará al Grupo de Respuesta a Incidentes TIC y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de los sistemas de información.

• Coordinar sus actuaciones con el Departamento de Protección de Datos y Seguridad de la Información y colaborar con este en todos aquellos aspectos que puedan incidir en las competencias atribuidas a dicho Departamento.

Por su parte, el artículo 32 del citado Reglamento establece que el **Comité de Seguridad TIC** es el órgano que gestiona y coordina la Seguridad de los sistemas de información TIC a nivel de organización. Específicamente le corresponde:

• Coordinar todas las funciones de seguridad de los sistemas de información TIC de la Corporación.

• Velar por el cumplimiento de la legislación y normativa interna de aplicación.

• Recabar del Responsable de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes se consolidan y resumen para la Dirección de la Corporación.

• Atender las peticiones de información que pueda requerir el Departamento de Protección de Datos y Seguridad de la Información, así como las recomendaciones y propuestas efectuadas por dicho Departamento.

• Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad.

• Dinamizar la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas de información, promoviendo inversiones de carácter horizontal.

• Designar a los componentes del Grupo RITIC indicado en el artículo 15 de la presente disposición.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones, así como reclamar la presencia del citado personal en sus sesiones o su incorporación a las comisiones delegadas de trabajo que pudieran constituirse.

Por último, el artículo 35 del referido Reglamento atribuye al **Departamento de protección de datos y seguridad de la información** una serie de competencias y responsabilidades. Específicamente en materia de seguridad de la información le corresponde:

• Elaborar el Plan general Auditor de Protección de Datos personales y Seguridad de la Información de la Diputación y llevar a cabo las actuaciones auditoras en él comprendidas que le correspondan.

• Ejecutar la Auditoría de la seguridad de los sistemas de información a la que se refiere el Esquema Nacional de Seguridad.

• Supervisar el cumplimiento de la normativa legal e interna en materia de seguridad de la información.

• Llevar a cabo investigaciones sobre hechos e incidentes de seguridad de la información.

• Elaborar estudios, propuestas de regulación, documentos para facilitar el cumplimiento normativo y evacuar consultas e informes en la materia.

• La difusión de todo tipo de información y la organización de actividades que fomenten el conocimiento, el cumplimiento normativo y las buenas prácticas en materia de seguridad de la información, tanto en el entorno corporativo como en la sociedad en general.

Todos los empleados de la Corporación están obligados a facilitar cuanta información le sea requerida por el departamento de Protección de Datos y Seguridad de la Información, así como el acceso a locales, instalaciones, equipos, archivos, soportes de almacenamiento, programas, procesos y procedimientos.

N/SEG/USU-010 INFORMACIÓN, DIFUSIÓN Y FORMACIÓN

En virtud de lo dispuesto en el artículo 42 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, la Corporación debe garantizar la formación y concienciación a todos sus empleados públicos en materia de seguridad de la información.

El objetivo general de dichas acciones es evitar que los empleados públicos puedan incurrir en la conculcación de los preceptos establecidos por la normativa de seguridad de la información.

A tal efecto, y como objetivos específicos, las actuaciones irán dirigidas a:

• Informar al personal de la normativa legal e interna que regula la seguridad de la información, los deberes y responsabilidades que impone, y las consecuencias que puede comportar su incumplimiento.

• Formar al personal en los conocimientos y las habilidades profesionales necesarios para la correcta aplicación de las políticas y procedimientos internos en la materia, así como en el manejo de las herramientas técnicas que la organización implante para la gestión y cumplimiento.

• Mentalizar al personal de la necesidad de incorporar a los procesos habituales de trabajo las previsiones en materia de seguridad de la información.

• Mantener actualizado al personal en los posibles cambios legislativos y/o de la normativa interna en materia de seguridad de la información.

N/SEG/USU-010-1 INFORMACIÓN Y DIFUSIÓN

Deberá habilitarse un espacio en la *intranet* corporativa en el que todos los empleados tengan acceso al conjunto de normativas internas relativas a la seguridad de la información. En la medida de lo posible, se utilizará también

dicho espacio para la inclusión de todos aquellos recursos que la Diputación disponga para facilitar la gestión y cumplimiento en la materia. El Departamento de Protección de Datos y Seguridad de la Información será el responsable de dar contenido y administrar el citado espacio.

Podrán utilizarse cualesquiera otros instrumentos o cauces que el Departamento de Protección de Datos y Seguridad de la Información estime oportunos para lograr el objetivo de información para aquellos colectivos o centros que, en atención a sus especiales circunstancias, no tengan asegurado el acceso al espacio en la *intranet* anteriormente descrito.

Con independencia de lo previsto en los párrafos anteriores, el personal directivo al frente de los diferentes departamentos y unidades deberá proceder a dar la mayor difusión posible a las normativas y recursos citados entre el personal de su ámbito de dirección.

El Servicio de Recursos Humanos procederá a incluir en los documentos relativos a las nuevas incorporaciones y renovaciones de personal una referencia a las obligaciones y responsabilidades que se adquieren en materia de seguridad de la información.

N/SEG/USU-010-2 ACTIVIDADES FORMATIVAS

Las actividades formativas se llevarán a cabo conforme lo dispuesto en el artículo 42 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia.

El personal directivo al frente de los diferentes departamentos y unidades organizarán debidamente sus recursos humanos para que su personal dependiente perfeccione las acciones formativas correspondientes.

N/SEG/USU-011 INCUMPLIMIENTOS

Al personal al servicio de la Diputación de Valencia que incumpla lo previsto en la presente normativa le será de aplicación el régimen disciplinario establecido por la legislación vigente para el personal al servicio de la administración pública que resulte de aplicación, sin perjuicio de que los hechos puedan ser constitutivos de responsabilidades en otro orden.

Cuando los incumplimientos fuesen cometidos por terceros, sobre los que recaiga la obligación de cumplimiento en virtud de contrato o cualquier otro tipo de relación acordada, la responsabilidad les será exigida en los términos previstos en los instrumentos que regulen dichas relaciones y por la normativa legal que pueda resultar de aplicación.

En el supuesto de que un usuario no observe alguno de los preceptos señalados en la presente normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.