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 de la Diputación Provincial de Valencia)

NORMAS DE SEGURIDAD PARA EL PERSONAL TÉCNICO DE LOS SISTEMAS DE INFORMACIÓN TIC

CÓDIGO	N/SEG/TEC	**APROBACIÓN**	Decreto nº 967, de 18 de enero de 2023, 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
18/01/2023	01	01	Aprobación inicial de la norma

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

FECHA DE EMISIÓN: Enero 2023

INDICE

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 num 967, de 18 de enero de 2023, el Presidente de la Diputación de Valencia ha aprobado las presentes *Normas de Seguridad para el Personal Técnico de los Sistemas de Información TIC.*

En el presente documento consta la normativa interna relacionada con la seguridad de los sistemas de información TIC de la Diputación de Valencia que deben cumplir los técnicos de dichos sistemas de información. En consonancia con el artículo 4 del citado Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal, la presente normativa es de aplicación a los departamentos en que se integre el personal técnico de los sistemas de información TIC, y resultará de obligado cumplimiento para todo el citado personal técnico.

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, las *Normas de Seguridad de los Usuarios de los Sistemas de Información*, aprobadas por Decreto nº 15873, de 27 de diciembre de 2022, del Presidente de la Diputación de Valencia y lo recogido en el siguiente glosario:

a) ***Acceso remoto****: Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.*

b) ***Administradores de seguridad delegados****: Quienes por delegación del Administrador de Seguridad de los Sistemas de Información TIC asumen, en el ámbito de sus competencias funcionales, determinadas atribuciones de dicho Responsable (art*. 30 Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal)*.*

c) ***Bastionado de seguridad****. El bastionado o configuración de seguridad comprende el conjunto de técnicas que buscan mejorar el nivel de seguridad de un sistema sin alterar la capacidad para desempeñar su labor.*

d) ***CMDB*** *(Siglas en inglés de base de datos de la gestión de configuración): La CMDB es un repositorio de información donde se relacionan todos los componentes de un sistema de información, ya sean hardware, software, documentación, etc.*

e) ***Computación en la nube (cloud computing)****: La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio. [NIST SP-800-145]*

f) ***Contraseña****: Información confidencial, a menudo compuesta de una cadena de caracteres, que puede ser usada en la autenticación de un usuario, entidad o recurso.*

g) ***Declaración de Aplicabilidad****: Documento formal firmado por el Responsable de Seguridad de los Sistemas de Información donde constan las medidas de seguridad que deben implementarse en un sistema de información.*

h) ***Desastre:*** *Se entiende por desastre cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.*

i) ***Dominio de seguridad****: Conjunto de sistemas de información sometidos a una Política de Seguridad común, es decir, homogéneos desde el punto de vista de las medidas de seguridad que hay que aplicar.*

j) ***Firewall (cortafuegos)****: Aquél sistema formado por aplicaciones, dispositivos o combinación de estos, encargado de hacer cumplir una política de control de acceso en las comunicaciones entre dispositivos de red según una política de seguridad existente.*

k) ***Interconexión de sistemas de información****: Se produce una conexión cuando se proveen los medios físicos y lógicos de transmisión adecuados y susceptibles de ser empleados para el intercambio de información. Se produce una interconexión de sistemas cuando existe una conexión y se habilitan flujos de comunicación entre los mismos.*

l) ***Responsables de Seguridad delegados****: Quienes por delegación del Responsable de Seguridad de los Sistemas de Información asumen, en el ámbito de sus competencias funcionales, determinadas atribuciones de dicho Responsable (art*. 28 Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal).

m) ***Responsables del Sistema delegados****: Quienes por delegación del Responsable de los Sistemas de Información TIC asumen, en el ámbito de sus competencias funcionales, determinadas atribuciones de dicho Responsable (art*. 29 Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal).

2. NORMATIVA INTERNA DE SEGURIDAD PARA EL PERSONAL TÉCNICO DE LOS SISTEMAS DE INFORMACIÓN TIC

A los efectos de la presente normativa se considera **personal técnico de los sistemas de información TIC** a toda persona cuyo cometido profesional consista en el análisis, diseño o desarrollo de proyectos tecnológicos, la programación, mantenimiento, soporte técnico y gestión de los diferentes componentes tecnológicos de los sistemas de información TIC. Se incluye también el personal con atribuciones o responsabilidades profesionales en materia de seguridad de los sistemas de información TIC.

En la presente normativa se establecen las directrices generales de seguridad que implican al personal técnico, lo cual no agota ni restringe el entorno de seguridad de los sistemas de información TIC, sino que completa al resto de disposiciones normativas internas de la Diputación de Valencia que, elaboradas también con el objetivo de la seguridad de dichos sistemas, vayan dirigidas a otros perfiles de destinatarios.

De conformidad con lo dispuesto en el artículo 3 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia, las presentes normas son de aplicación a todos los sistemas de información TIC que sean de la titularidad de la Diputación de Valencia o cuya gestión o responsabilidad tenga encomendada.

N/SEG/TEC-001 ENTORNO DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN TIC

El entorno de seguridad de los sistemas de información TIC comprende el conjunto de medidas de carácter técnico y organizativo que resultan de

aplicación para preservar la seguridad de los diferentes elementos o activos que integran dichos sistemas.

N/SEG/TEC-001-1 MEDIDAS DE SEGURIDAD

Las **condiciones básicas de seguridad** que deberán estar presentes en **todos los sistemas de información** serán:

- Los principios básicos y requisitos mínimos de seguridad recogidos en el Esquema Nacional de Seguridad.

- Las medidas de seguridad de los artículos y del Anexo II del Esquema Nacional de Seguridad establecidas para los sistemas de información de categoría BÁSICA y que afecten a todas las dimensiones de seguridad.

- En el ámbito de la protección de datos personales, se atenderá a lo dispuesto en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Una vez establecida la seguridad básica y tras la evaluación del sistema, será necesario implementar aquellas medidas de seguridad correspondientes a la categoría del sistema.

La seguridad también podrá verse incrementada, una vez mejorada, en aquellos supuestos que así lo reclame la criticidad de un sistema de información, 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.

Corresponde al **Responsable de Seguridad de los Sistemas de Información** determinar las medidas de seguridad concretas para cada sistema de información, de acuerdo con la normativa de aplicación, así como la supervisión sistemática y periódica de las medidas implementadas. Las condiciones concretas de seguridad se plasmarán en la correspondiente **Declaración de Aplicabilidad.**

Las condiciones de seguridad establecidas en la Declaración de Aplicabilidad se implementarán en cada sistema de información afectado. Será obligación de cada **responsable del sistema delegado** asegurar que los requisitos de seguridad se integran adecuadamente en su ámbito, y de los **administradores de seguridad delegados** la responsabilidad de llevar a cabo su implantación, gestión y mantenimiento.

Cuando alguna medida de seguridad o salvaguarda comporte especial dificultad en su implementación, a juicio de los administradores de seguridad delegados afectados, éstos deberán realizar un estudio del alcance y la viabilidad técnica y económica de la implementación. Con este informe el Comité de Seguridad TIC deberá decidir la fórmula de ejecución más viable y el plazo para llevarla a cabo, considerando los recursos necesarios.

Una vez que dicha medida o salvaguarda se encuentre implantada y plenamente operativa, el Administrador de Seguridad delegado afectado emitirá una Declaración en la que conste su entrada en funcionamiento.

Deberá elaborarse un procedimiento en el que se establezcan las pautas de actuación para garantizar que al Responsable de Seguridad de los Sistemas de Información le llega la información necesaria para poder determinar las medidas de seguridad concretas que son de aplicación a cada sistema de información,

así como que ningún sistema de información entre en operación sin adoptar las medidas de seguridad que le sean de aplicación.

N/SEG/TEC-001-2 ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

A los efectos de valoración de riesgos, se determinarán en cada sistema los activos más valiosos y sus amenazas más probables.

Cada responsable, respecto de sus activos, deberá:

- Incorporar cada elemento nuevo al inventario, proporcionando la información pertinente y establecimiento las dependencias entre activos.
- Mantener la información del activo actualizada.
- Llevar a cabo la valoración de riesgos.

N/SEG/TEC-001-3 SEGURIDAD EN SERVICIOS DE TERCEROS

El entorno de seguridad de los sistemas de información que resulte de aplicación lo será con independencia de que se recurra a la contratación de servicios externos. La responsabilidad del cumplimiento de las condiciones de seguridad de todo o parte de un sistema de información de la Diputación de Valencia corresponde exclusivamente a ésta y no puede ser transferida a terceros, por lo que se dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento. Para ello, el personal técnico que participe en la contratación de este tipo de servicios atenderá lo previsto en el apartado N/SEG/TEC-021-2.

Cuando se trate de supuestos de *cloud computing* se estará, además, a lo previsto en el apartado N/SEG/TEC-010.

En caso de que se utilicen plataformas, programas o servicios **bajo el control y gestión de otro organismo público** –diferente dominio de seguridad- como parte de los recursos (activos) para prestar un servicio y/o explotar una información, deberá formalizarse con dicho organismo un convenio o acuerdo en el que conste el marco general de seguridad a aplicar y la responsabilidad de cada entidad pública.

N/SEG/TEC-001-4 SEGURIDAD EN INTERCONEXIÓN DE SISTEMAS DE INFORMACIÓN

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Previamente a la interconexión de los sistemas:

- Se documentará la necesidad de interconexión y se hará constar: las características de la interfaz, los requisitos de seguridad y protección de datos, la naturaleza de la información intercambiada y el tipo de información que se requiere intercambiar entre ambos sistemas.
- La interconexión deberá autorizarse por el Responsable de los Sistemas de Información.

- La interconexión estará sujeta al análisis y gestión de riesgos de la seguridad. Un aumento en el nivel de riesgo a causa de la interconexión requerirá un informe del Responsable de Seguridad de los Sistemas de Información.

La interconexión de dos sistemas se realizará mediante un Sistema de Protección de Perímetro (SPP). Este SPP será una combinación de recursos *hardware* y/o *software*, que será denominado Dispositivo de Protección de Perímetro (DPP), cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los sistemas.

Deberá elaborarse un procedimiento para la interconexión de los sistemas, donde se establezcan las especificaciones técnicas del entorno de seguridad de sistemas interconectados.

N/SEG/TEC-001-5 SEGURIDAD DE COMUNICACIONES, NOTIFICACIONES Y PUBLICACIONES ELECTRÓNICAS

Las comunicaciones electrónicas a las que se refiere la Ley 39/2015 (PAC) adoptarán las condiciones de seguridad previstas en la presente normativa que resulten apropiadas para garantizar:

- La constancia de la transmisión y recepción de la comunicación electrónica, de las fechas en las que se realizaron, así como del contenido íntegro de las mismas.
- La identificación fidedigna del remitente y destinatario de la comunicación.

De igual forma, las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos adoptarán las condiciones de seguridad previstas en la presente normativa que resulten apropiadas para:

- Asegurar la autenticidad del organismo que lo publique.
- Asegurar la integridad de la información publicada.
- Dejar constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.
- Asegurar la autenticidad del destinatario de la publicación o notificación.

N/SEG/TEC-002 PLANTEAMIENTO INTEGRAL DE LA SEGURIDAD

Se dispondrá de un conjunto de documentos aprobados por el Comité de Seguridad TIC referidos al planteamiento integral de la seguridad del sistema. La documentación elaborada a estos efectos será, como mínimo, la siguiente:

a) Documentación de las instalaciones. Se detallarán las instalaciones, precisando:

- La clasificación de la instalación, atendiendo a lo dispuesto en el apartado N/SEG/TEC-017
- Las áreas existentes
- Los puntos de acceso

b) Documentación del sistema. Se dispondrá de un inventario actualizado del sistema de información. El inventario contendrá una descripción:

- De los equipos
- De las redes internas existentes, y los elementos de conexión al exterior
- De los puntos de acceso al sistema

- De los responsables de los elementos; entendiendo como responsable a la persona que es responsable de las decisiones relativas a cada elemento

c) Documentación de líneas de defensa. Se dispondrá de un inventario con un esquema de los sistemas de seguridad del sistema de información. El inventario contendrá una descripción:

- De los elementos de interconexión a otras redes
- De los elementos de defensa en las conexiones a otras redes
- De las posibles tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa

d) Documentación del sistema de identificación y autenticación de usuarios. Se detallarán los sistemas de identificación y autenticación de usuarios para cada sistema o servicio. Se precisarán:

- El mecanismo de autenticación a cada sistema o servicio
- Dónde se almacenan las contraseñas

e) Documentación de los controles técnicos internos. Se detallará cómo se controlan los datos una vez en los sistemas. Se describirá la validación de datos de entrada, salida y datos intermedios

f) Documentación del sistema de gestión con actualización y aprobación periódica. Se detallará cómo se gestionan los elementos antes enumerados, con qué frecuencia se revisan, quién es el encargado de la tarea y quién es el responsable de su aprobación.

N/SEG/TEC-003 AUTORIZACIONES

Sin perjuicio de otras referencias de autorización recogidas en esta u otra normativa interna, se expresan a continuación para cada uno de los siguientes tipos de componente o actuación del sistema de información, la persona o punto de contacto para su autorización:

a) Corresponde al **Responsable de los Sistemas de Información** o **Responsable del Sistema delegado** la autorización para:

- La utilización de instalaciones, tanto habituales como alternativas.
- La entrada de equipos en producción, en particular, equipos que involucren criptografía.
- La instalación en el sistema de cualquier elemento físico o lógico.
- La entrada de aplicaciones en producción.
- La recuperación de información de las copias de seguridad, en los casos en que no sea a solicitud de los usuarios de la información.

b) Corresponde al **Responsable de los Sistemas de Información** o **Responsable del Sistema delegado**, previa autorización del **Responsable de la Información o del Servicio correspondiente,** la autorización para:

- El acceso de una entidad (usuario o proceso) al sistema de información.
- La utilización de equipos portátiles y móviles.
- La utilización de medios de comunicación, habituales y alternativos.
- La recuperación de información de las copias de seguridad, cuando sea a solicitud de los usuarios de la información.

Todo proceso de autorización estará debidamente documentado, debiendo existir un modelo de solicitud (formulario) que contenga la información necesaria para que el responsable pueda tomar la decisión sobre la autorización de manera adecuada.

N/SEG/TEC-004 ACCESO LÓGICO

N/SEG/TEC-004-1 CONTROL DE ACCESO

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda acceder, o no, a un recurso del sistema para realizar una determinada acción.

El acceso lógico y operativo a los sistemas de información de la Diputación de Valencia se controlará a través del software de seguridad de acceso a la red, así como a través de los módulos de seguridad de las aplicaciones específicas.

Los accesos al sistema respetarán, en cualquier caso, los siguientes principios:

a) **Mínimo privilegio**. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.
b) **Necesidad de conocer**. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
c) **Capacidad de autorizar**. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Se dispondrá de mecanismos para el control de todos los accesos (usuarios o procesos) al sistema de información, sean locales o remotos. Estos mecanismos deberán garantizar:

- Que todo acceso esté prohibido salvo concesión expresa, de forma que se impida su utilización salvo a las entidades que disfruten de derechos de acceso suficientes. Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

- Que un usuario no pueda acceder a recursos con derechos distintos de los autorizados.

- Que cada entidad (usuario o proceso) que accede al sistema tiene un identificador singular, que permita saber quién ha hecho algo y qué ha hecho.

- Que se definan para cada entidad a qué se necesita acceder, con qué derechos y bajo qué autorización.

- La existencia de una relación del personal autorizado para conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por la normativa interna.

- La existencia de un registro de las entidades responsables de cada identificador, que permita saber a quién corresponde cada identificador y los permisos o derechos que tiene, así como quién ha sido su autorizante.

- La inhabilitación del identificador cuando el usuario deja la organización, cesa en la función para la cual se requería la cuenta de usuario o cuando la persona que la autorizó da orden en sentido contrario.

• Que, no obstante la inhabilitación anterior, el identificador se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a los mismos (período de retención).

• La segregación de funciones y tareas críticas en los sistemas críticos y en los de categoría MEDIA o superior, de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita. Como mínimo serán incompatibles: Desarrollo con operación del sistema, configuración y mantenimiento del sistema con operación del sistema, auditoría o supervisión del sistema con cualquier otra función.

Ningún usuario final deberá tener privilegios especiales que le permitan configurar parámetros de seguridad o administrar claves.

El acceso a las aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.

Para minimizar el número de accesos no autorizados a los sistemas se tendrán en cuenta los aspectos siguientes:

• Hasta que no se haya completado con éxito el proceso de autenticación, no se deberá mostrar ningún tipo de información relativa al sistema que pueda ayudar a identificarlo, así como cualquier otro tipo de información que pueda facilitar su acceso no autorizado.

• Una vez se haya accedido correctamente al sistema, se deberá mostrar un mensaje que advierta que el uso del sistema sólo está permitido a usuarios autorizados.

• La validación de la información de entrada se realizará únicamente cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no deberá indicar en ningún caso la parte del dato que es incorrecta.

• Siempre que sea posible, deberán utilizarse protocolos de comunicación que permitan el envío de las credenciales de usuario de forma cifrada para evitar que sean capturadas en algún punto intermedio de la comunicación.

N/SEG/TEC-004-2 ACCESO REMOTO

En los accesos remotos se observarán las mismas condiciones que las señaladas para el acceso local y se protegerá el canal de acceso remoto con las medidas indicadas en el apartado N/SEG/TEC-006 para la protección de las comunicaciones.

El Comité de Seguridad TIC decidirá qué actividades pueden realizarse remotamente, así como aquellas que requieran de autorización previa, quién puede autorizarlas y, en su caso, el período de autorización. De todo ello se dejará constancia en los procedimientos pertinentes.

A fin de limitar lo que se puede hacer en remoto se deberá establecer un filtro, bien en el servidor, bien en el equipo cliente.

N/SEG/TEC-004-2-1 TELETRABAJO

Las directrices recogidas en el presente apartado son complementarias de las disposiciones contenidas en el apartado 2-002-11 MODALIDAD DE TELETRABAJO de las Normas de Seguridad para los usuarios de los Sistemas de Información, aprobadas por Decreto nº 15873 de 27 de diciembre de 2022 del Presidente de la Diputación de Valencia.

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 el Servicio de Informática.

El Servicio de Informática entregará las credenciales de acceso para que los usuarios puedan acceder a través de las diferentes opciones que se ofrecen en la modalidad de teletrabajo.

El Servicio de Informática suministrará el equipamiento y las aplicaciones informáticas que resulten adecuadas para la prestación del servicio bajo la modalidad de teletrabajo.

Este equipamiento de aplicaciones informáticas las realizará a través de tres métodos:

- Webs corporativas: Web de accesos a través de internet, donde no se requerirá ninguna característica especial en los equipos, solamente se utilizará el usuario-contraseña y Múltiple Factor de Autenticación (MFA) que la organización utilice.

- Citrix: Entorno dónde se utilizará un listado de aplicaciones publicadas, diferentes para cada usuario en función de sus roles o autorizaciones dadas por los responsables de la organización.

En esta opción será necesario disponer de aplicaciones informáticas instaladas en el equipo para poder conectar al entorno de Citrix mediante usuario-contraseña y MFA.

- VPN: Entorno donde se realizará la conexión mediante protocolo VPN hacia el organismo. Este entorno deberá de ser autorizado por el personal responsable de los diferentes departamentos.

El equipamiento informático y las aplicaciones informáticas suministradas serán de uso exclusivamente laboral. Asimismo, la Diputación de Valencia suministrará un número de teléfono IP o móvil corporativo de acuerdo a la peculiaridad de las funciones y tareas del puesto.

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.

Corresponderá a la persona teletrabajadora 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.

Asimismo, 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.

La Diputación de Valencia deberá dotar a las personas que desarrollen su actividad bajo la modalidad de teletrabajo de un servicio informático de apoyo técnico para la resolución de incidencias puntuales.

El personal en esta modalidad deberá de custodiar los activos que la organización le preste para el desarrollo de su trabajo, por lo que deberá seguir las indicaciones de seguridad recogidas en la normativa interna en la materia.

El tráfico deberá ser cifrado mediante configuraciones y criptología que haya sido definida por cualquier guía o manual de bastionado, ya sea de fabricante, del CCN, CIS o NIST.

Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.

Deberán recogerse registros de auditoría de este tipo de conexiones

Deberá de utilizarse guías o manuales de configuración para establecer un bastionado de los activos, refiriéndose por activo, cualquier activo que forme parte del proceso de acceso remoto, tanto de activos perimetrales, internos, concienciación del personal, como dispositivos móviles, así como seguir la estrategia de seguridad de acceso remoto que se haya establecido en el organismo.

N/SEG/TEC-004-3 IDENTIFICACIÓN DE USUARIOS

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

Las cuentas de usuario se gestionarán de la siguiente forma:

- Cada cuenta estará asociada a un identificador único.
- Las cuentas deben ser inhabilitadas en los siguientes casos: Cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario. Se automatizarán al máximo posible las tareas que permitan la inhabilitación inmediata de las cuentas cuando se produzcan las circunstancias de inhabilitación.

Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención. Los períodos de retención serán determinados por el Comité de Seguridad TIC.

La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.

Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

N/SEG/TEC-004-4 MECANISMOS DE AUTENTICACIÓN

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán **credenciales**. En los sistemas de información TIC de la Diputación de Valencia podrán utilizarse los siguientes factores de autenticación:

a) Algo que se sabe. Contraseñas o claves concertadas.

b) Algo que se tiene. Componentes lógicos o dispositivos físicos.

c) Algo que se es. Elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

En aquellos sistemas no críticos y de categoría BÁSICA, como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor. Se exigirá el uso de al menos dos factores de autenticación cuando se trate de sistemas críticos o de categoría MEDIA y superior.

En sistemas de categoría MEDIA no está aconsejado el uso de claves concertadas, en el caso de utilización se permitirán aquellas que estén formadas

de al menos 8 caracteres alfanuméricos. Si estos últimos son generados de forma aleatoria o pseudoaleatoria, deberán poseer la suficiente seguridad como para evitar repeticiones o hipótesis acerca de su posible valor. El uso de claves concertadas no se permitirá en sistemas críticos o de categoría ALTA.

Cuando se trate de sistemas críticos o de categoría ALTA los mecanismos de autenticación se basarán en dispositivos físicos personalizados o mediante dispositivos que hagan uso de patrones biométricos. En el caso de utilizar un patrón biométrico se requerirá la utilización de un segundo factor de autenticación *token* o clave segura (generada de forma aleatoria y con una longitud de al menos 8 caracteres alfanuméricos). En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos *hardware* usando algoritmos y parámetros acreditados por el CCN.

Para dar seguridad a las credenciales se atenderá, como mínimo, a lo siguiente:

Las credenciales se activarán una vez estén bajo el control efectivo del usuario.

Las credenciales estarán bajo el control exclusivo del usuario.

El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

Las credenciales se cambiarán con la periodicidad marcada por el Comité de Seguridad TIC, atendiendo a la categoría del sistema y al resultado del análisis de riesgos. De igual modo, las credenciales se suspenderán tras un periodo de no utilización definido por el Comité.

Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema o cuándo la persona que lo autorizó dé la orden en sentido contrario.

Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración.
Se contemplan varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la Ley 39/2015 (LPAC).

El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o, Se emplearán certificados cualificados como mecanismo de autenticación y este, estará protegido por un segundo factor, del tipo PIN o biométrico.

Se registrarán los accesos con éxito y los fallidos.

Se informará al usuario del último acceso efectuado con su identidad.

N/SEG/TEC-004-5 USO DE CONTRASEÑAS

Sin perjuicio de lo establecido en el apartado anterior “mecanismos de autenticación”, cuando el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios consista en contraseñas, se cumplirán las siguientes condiciones:

Las contraseñas, mientras estén vigentes, se almacenarán con algún método de protección que garantice su confidencialidad e integridad; es decir, de forma ininteligible, que no se pueda entender.

La clave o identificación de acceso, otorgada por el Servicio de Informática en el momento del alta del usuario, le será comunicada de manera segura. No deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica no seguros, ni comunicadas por teléfono. Es responsabilidad del usuario efectuar los cambios de la misma, de acuerdo con la periodicidad y sintaxis establecida. Se podrá establecer un sistema de generación automática de claves de acceso con las debidas garantías de seguridad.

La contraseña facilitada al usuario por el Servicio de Informática será provisional y deberá forzar su cambio inmediato, tras el primer inicio de sesión, por otra personalizada por el usuario.

El usuario podrá efectuar el cambio voluntario de la clave siempre que lo desee. De igual forma, el administrador del sistema, aplicación o producto utilizado por el usuario, podrá efectuar el cambio de clave si se produce alguna incidencia que aconseje dicho cambio.

En el momento del cambio, no estará permitida la re-utilización del valor empleado para las últimas claves, según la antigüedad que se especifique.

• La clave del usuario no deberá ser mostrada en pantalla mientras se introduce.

• Las contraseñas para que sean válidas deberán tener una longitud mínima de seis posiciones y consistir en una combinación de caracteres alfanuméricos.

• Se debe evitar la característica “Recordar Contraseña” existente en algunas aplicaciones y formularios.

• Las contraseñas deberán forzar su cambio periódicamente. Deben existir mecanismos de expiración y caducidad de contraseñas para obligar a los usuarios al cambio de la misma.

• Se establecerá un número de intentos de acceso fallidos. Una vez superado éste se producirá el bloqueo automático del usuario.

• Las decisiones sobre límite de intentos de acceso fallidos, la periodicidad para el cambio de contraseñas y la política de calidad de las contraseñas serán adoptadas por el El Comité de Seguridad TIC atendiendo a la categoría del sistema y al resultado del análisis de riesgos. El producto de dichas decisiones se documentará a través del procedimiento para la asignación, distribución y almacenamiento, en su caso, de los mecanismos utilizados para la identificación y autenticación en los sistemas de información.

• Todas las contraseñas por defecto de los sistemas o aplicaciones deben ser cambiadas cuando no sean necesarias.

• Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación según guías CCN-STIC

• El Comité de Seguridad TIC decidirá sobre la oportunidad de que ciertos usuarios puedan utilizar programas gestores de contraseñas.

N/SEG/TEC-005 MONITORIZACIÓN

La monitorización es la actividad consistente en la recopilación de información, a través de *software* u otro tipo de mecanismos sensores, del entorno de un sistema de información para su posterior análisis, control o simple obtención de evidencias.

Todos los equipos que cuenten con un reloj interno estarán sincronizados entre sí para garantizar la precisión de los sucesos registrados y permitir la correlación de los diferentes eventos.

Aquellos sucesos registrados que puedan ser susceptibles de constituir evidencias en procesos judiciales o en procedimientos administrativos sancionadores, deberán contar con todas aquellas garantías tecnológicas que proporcionen el carácter de prueba válida a dichos sucesos.

N/SEG/TEC-005-1 REGISTROS DE ACTIVIDAD

Deberán existir, como mínimo, los siguientes tipos de registros de actividad:

a) **Registro de actividad de usuarios en el sistema**. Se registrarán las actividades de los usuarios en el sistema, de forma que el registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información. Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema. Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.

La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema.

El registro de actividad irá asociado a la cuenta de usuario en los casos a que se refiere el apartado N/SEG/TEC-004-1.

b) **Registro de accesos a tratamientos de datos personales pertenecientes a categorías especiales o con riesgo alto**. En todos aquellos tratamientos de datos personales de pertenecientes a las categorías especiales o aquellos que arrojen un resultado de un riesgo alto según el análisis de riesgos, deberá habilitarse un registro automático de todos los accesos, aunque el intento de acceso no haya tenido éxito. Dicho registro contendrá, como mínimo, la siguiente información: La identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. El Responsable de Seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. El período mínimo de conservación de los datos registrados será de **dos años**.

c) **Registro de evidencias de actividad en un procedimiento sancionador administrativo o en un proceso judicial**. Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, tanto a nivel operativo como de administración, permitiendo identificar en cada momento a la persona que actúa. Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o

hacer frente a ella, cuando un incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

El Comité de Seguridad TIC podrá acordar la creación de otros registros de actividad si así lo estima conveniente.

El Delegado de Protección de Datos y el Departamento de Protección de Datos y Seguridad de la Información, en el ejercicio de sus competencias, siempre tendrán acceso a los registros descritos en los apartados anteriores y a cualesquiera otros que puedan crearse a criterio del Comité de Seguridad TIC.

El sistema se configurará de forma que el contenido de dichos registros no pueda modificarse, así como la garantía de protección ante la eliminación por personas no autorizadas. En cualquier caso, y puesto que también se recoge la actividad de los operadores y administradores del sistema, se garantizará que los propios operadores y administradores no puedan modificarlos o eliminarlos.

Cuando se trate de los registros descritos en los apartados b) y c), se configurarán de manera que su eliminación requiera el concurso de dos personas: El Responsable de Seguridad de los Sistemas de Información y el Responsable de los Sistemas de Información. Deberá dejarse constancia documental de cada eliminación del contenido de dichos registros.

Los mecanismos que permiten los registros de los apartados b) y c) estarán bajo el control directo del Responsable de Seguridad de los Sistemas de Información sin que deban permitir la desactivación ni la manipulación de los mismos. De igual modo, el acceso a los citados registros y su custodia corresponderán al Responsable de Seguridad de los Sistemas de Información, a excepción de lo dispuesto en este mismo apartado respecto de las competencias del Delegado

de Protección de Datos y el Departamento de Protección de Datos y Seguridad de la Información.

Se elaborará un inventario de los registros de actividad, donde además se indicará el personal autorizado a su acceso o eliminación. Y el período de retención de los mismos.

Se dispondrá de un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención, así como de un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad. Las copias de seguridad se ajustarán a los mismos requisitos establecidos para los registros en vivo.

N/SEG/TEC-005-2 MONITORIZACIÓN OPERATIVA DE LA SEGURIDAD

Deberán establecerse las rutinas de operación de la seguridad que permitan la prevención, detección y corrección temprana de posibles incidentes de seguridad, así como monitorizar, detectar e informar automáticamente cuando una norma o política de seguridad haya sido violada, tal como los cambios en la configuración de seguridad aprobada previamente. La aplicación de esta norma deberá desencadenar, siempre que sea posible, acciones automáticas.

A efectos de seguridad, deberá hacerse uso de la monitorización del tráfico de red con dos grandes objetivos: Primero, para detectar situaciones anómalas que puedan introducir riesgos en la seguridad corporativa y, segundo, dentro de la gestión de un incidente, para identificar las actividades a través de la red de un intruso o un software dañino concreto.

Se utilizará la monitorización del tráfico de red con los siguientes objetivos específicos:

• Estudiar la información transmitida a través de un protocolo para identificar la criticidad de la información enviada por la red y aplicar así salvaguardas en caso de ser requeridas.

• Comprobar el tipo de información que puede ser observada por otro usuario con posibilidad de conectarse a la misma red para identificar los riesgos de robo de datos a los que nos exponemos.

• Definir perfiles de tráfico que nos permitan identificar anomalías en la red.

• Identificar tráfico no conocido por los administradores de la red y determinar si es o no legítimo.

• Investigar un posible incidente o investigar el tráfico relacionado con un incidente de seguridad confirmado para proceder a realizar la respuesta adecuada (contención, erradicación…).

• Capturar información sensible.

Se seguirán las especificaciones contenidas en la Guía CCN-STIC-435 en lo que respecta al proceso de análisis de tráfico de red, selección e implantación de herramientas y contramedidas.

También se utilizará la monitorización del tráfico de host con el objetivo de prevenir ataques de escalado de privilegios.

El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

El acceso a las herramientas de captura y a los registros generados por las mismas, en especial a los ficheros de captura de tráfico, debe permanecer estrictamente restringido al personal que desempeñe las labores de monitorización. Adicionalmente, la protección de estos registros es vital para la organización, debido a la naturaleza de la información que pueden almacenar, por lo que deben desplegarse las medidas de seguridad necesarias en cada caso y eliminar los registros una vez hayan sido procesados.

N/SEG/TEC-005-3 MÉTRICAS E INDICADORES

Deberán establecerse mecanismos que permitan conocer en cada momento el estado de la seguridad, mejorarlo y gestionar los gastos e inversiones necesarios.

Las métricas e indicadores, que serán acordados por el Comité de Seguridad TIC, abarcarán los siguientes tipos:

- **De cumplimiento**. Para conocer el grado de cobertura de una cierta referencia (puede ser una política interna, un reglamento, un perfil, etc.).
- **De eficacia**. Para conocer el desempeño de una cierta función, desde el punto de vista de en qué medida logramos los resultados apetecidos.
- **De eficiencia**. Para conocer el desempeño de una cierta función, desde el punto de vista de si el consumo de recursos, en términos de horas y presupuestos, está proporcionado a los resultados obtenidos.

- **De impacto**. Para traducir los incidentes técnicos en consecuencias para la misión última del sistema: Protección de una cierta información y prestación de unos determinados servicios.
- **Predictivos**. Los indicadores que anticipan lo que va a pasar.
- **Explicativos**. Los que miden el pasado. Son útiles para entender lo que ha ocurrido y poder reaccionar con conocimiento de causa.

Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32 del ENS.

Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

N/SEG/TEC-006 PROTECCIÓN DE LAS COMUNICACIONES

N/SEG/TEC-006-1 SEGURIDAD PERIMETRAL Y FLUJOS DE INFORMACIÓN

Se dispondrá de un sistema de cortafuegos que separe la red interna del exterior, de modo que todo el tráfico con el exterior pase a través del cortafuegos. Sólo se permitirá el tráfico que haya sido previamente autorizado. El perímetro concreto, delimitado y acotado, estará reflejado en la arquitectura del sistema.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.
Se emplearán algoritmos y parámetros autorizados por el CCN para las conexiones.

Se emplearán, en el perímetro, tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

Para los flujos de información, el tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.

Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Los segmentos de red se implementarán por medio de redes de área local virtuales (Virtual Local Area Network, VLAN).

La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

• Usuarios.
• Servicios.
• Administración.

La protección deberá abarcar también los equipos de comunicaciones (*routers, switches*, etc). Es recomendable seguir las pautas recogidas en las guías CCN para reforzar la seguridad de estos elementos.

N/SEG/TEC-006-2 CONFIDENCIALIDAD, AUTENTICIDAD E INTEGRIDAD EN LAS COMUNICACIONES

Antes de intercambiar información alguna se asegurará la autenticidad del otro extremo de un canal de comunicación, tal como se establece en el apartado N/SEG/TEC-004.

Se dispondrá de mecanismos para la prevención de ataques activos, garantizando que al menos serán detectados y, en caso de ocurrir, la consiguiente activación de los procedimientos previstos de tratamiento del incidente. Se consideran ataques activos a aquellos ataques en los que se altere la información transmitida, se inserte información engañosa, o se secuestre la comunicación por una tercera parte.

Las comunicaciones que discurran por redes fuera del propio dominio de seguridad, en aquellos sistemas de categoría MEDIA y superior, utilizarán redes privadas virtuales (VPN), empleando protocolos estándar como IPSEC o TLS. Los equipos inalámbricos llevan incorporado mecanismos de cifrado de las comunicaciones, por lo que deberán ser configurados de forma segura empleando mecanismos actualizados. En cualquier caso, se implementará criptología correspondiente en las comunicaciones tal y como marque la guía CCN-STIC 807.

Hay que atender al secreto de las claves de cifra según lo indicado en N/SEG/TEC-014-3. En el caso de redes privadas virtuales, el secreto debe ser impredecible, mantenerse bajo custodia mientras dure la sesión y ser destruido al terminar. En el caso de otros procedimientos de cifrado, hay que cuidar de las claves de cifra durante su ciclo de vida en los términos recogidos en el apartado N/SEG/TEC-014-3.

Cuando se trate de sistemas críticos o de categoría ALTA se emplearán, preferentemente, dispositivos *hardware* en el establecimiento y utilización de la red privada virtual, de forma que las tareas de cifrado en los extremos se realicen en los equipos *hardware* especializados, evitando el cifrado por software. Los productos utilizados deberán estar certificados conforme a lo establecido en el apartado N/SEG/TEC-021-3.

De igual forma, cuando se trate de sistemas de categoría ALTA se llevará a cabo la segregación de redes. Se debe segmentar la red de forma que haya:

- Control (de entrada) de los usuarios que pueden trabajar en cada segmento, en particular si el acceso se realiza desde el exterior del segmento, tanto si es desde otro segmento de la red corporativa como si el acceso procede del exterior de la red, extremando las precauciones en este último escenario.
- Control (de salida) de la información disponible en cada segmento.
- Control (de entrada) de las aplicaciones utilizables en cada segmento.
- El punto de interconexión debe estar particularmente asegurado, mantenido y monitorizado.

No debería permitirse ningún protocolo directo entre los segmentos internos y el exterior, intermediando todos los intercambios de información.

Las redes se pueden segmentar por dispositivos físicos o lógicos.

N/SEG/TEC-007 OPERACIÓN DEL SISTEMA

La descripción detallada de cómo proceder a las tareas de operación y explotación del sistema se recogerá en los correspondientes procedimientos de

trabajo. Dichos procedimientos respetarán, en cualquier caso, lo dispuesto en este apartado.

N/SEG/TEC-007-1 CONFIGURACIÓN DE SEGURIDAD POR DEFECTO

Deberá realizarse una fortificación o bastionado del sistema de información previo a su entrada en operación de manera que se implemente una configuración segura por defecto; para esto deberán seguirse las guías CCN-STIC correspondientes, manteniendo la regla de “funcionalidad mínima” y “mínimo privilegio”, cubriendo al menos los siguientes aspectos:

a) Se retirarán las cuentas y contraseñas estándar.

b) Se desactivarán las funcionalidades técnicas no requeridas, ni necesarias, ni de interés o inadecuadas, ya sean gratuitas, de operación, administración o auditoría. Dichas funcionalidades quedarán documentadas y constará el motivo por el que se hayan deshabilitado.

c) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

d) Dispondrá de mecanismos que garanticen la corrección de la hora a la que se realiza el registro (de actividad, de incidencias, etc).

e) La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

f) Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.

g) Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.

h) Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

i) Se establecerán bloqueos de sesión por tiempo de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

j) Se habilitarán mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y "malware" en general) para todos los equipos (servidores y puestos de trabajo) Las opciones de configuración serán las recomendadas por el fabricante, así como las referentes a frecuencia de actualización; en caso contrario estará documentado el motivo.

k) Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.

l) Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.

m) Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.

n) Todo el sistema se escaneará regularmente para detectar código dañino.

o) Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

p) El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

q) El uso ordinario del sistema por los usuarios deberá ser sencillo y seguro. En caso de existir situaciones que puedan poner en riesgo la seguridad, y siempre que se trate de supuestos en que la organización la consienta bajo la responsabilidad del usuario, el sistema indicará esa posibilidad y las consecuencias al usuario, de forma que éste sea consciente de su exposición a un riesgo, debiendo el usuario dar su consentimiento expreso asumiendo el riesgo. De estos consentimientos informados de los usuarios quedará constancia en un registro.

Se dispondrá de un procedimiento documentado que indique la frecuencia y motivos por los que se debe modificar la configuración del sistema e incluirá: La aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema bajo la nueva configuración, y la retención de la configuración previa por un tiempo preestablecido.

N/SEG/TEC-007-2 DIMENSIONAMIENTO/GESTIÓN DE CAPACIDADES

En aquellos sistemas cuya dimensión de disponibilidad sea de nivel MEDIO o superior, ccon carácter previo a la adquisición o puesta en explotación de cualquiera de sus elementos se realizará un estudio previo que cubrirá los siguientes aspectos:

a) Necesidades de procesamiento.
b) Necesidades de almacenamiento de información: Durante su procesamiento y durante el periodo que deba retenerse.
c) Necesidades de comunicación.
d) Necesidades de personal: Cantidad y cualificación profesional.
e) Necesidades de instalaciones y medios auxiliares.
f) Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
g) Se emplearán herramientas y recursos para la monitorización de la capacidad.

N/SEG/TEC-007-3 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Se dispondrá de un plan de mantenimiento del equipamiento físico y lógico que indique la frecuencia, componentes a revisar, responsable de la revisión y evidencias a generar. Respecto a dicho plan de mantenimiento:

- Atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

- Contemplará mecanismos para el seguimiento continuo de los anuncios de defectos y un procedimiento documentado que indique quién y con qué frecuencia debe monitorizar esos anuncios, así como el procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

- El mantenimiento solo podrá realizarse por personal debidamente autorizado.

N/SEG/TEC-007-4 GESTIÓN DE CAMBIOS

Deberá mantenerse un control continuo de cambios realizados en el sistema. En tal sentido, se contará con un procedimiento de gestión de cambios, que indicará la frecuencia y motivos por los que se debe cambiar un componente del sistema e incluirá: La aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema tras el cambio, y la retención de una copia del componente previo por un tiempo preestablecido.

Respecto a dicho control de cambios:

- Analizará todos los cambios anunciados por el fabricante o proveedor para determinar su conveniencia para ser incorporados o no.

- Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.

- La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.

- Antes de poner en producción una nueva versión o una versión parcheada se comprobará en un equipo que no esté en producción (equivalente al de producción en los aspectos que se comprueban) que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.

• Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.

• Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

• Se planificarán los cambios para reducir el impacto sobre la prestación de los servicios afectados.

• Se determinará mediante análisis de riesgos si los cambios son relevantes para la seguridad del sistema. En caso de que el cambio implique una situación de riesgo de nivel alto deberá ser aprobado explícitamente de forma previa a su implantación.

N/SEG/TEC-007-5 OPERACIÓN DE HERRAMIENTAS DE SEGURIDAD

En general, se considerarán herramientas de seguridad el conjunto de *hardware* o *software* que proporcionan servicios orientados a reforzar y dar soporte a la seguridad de los sistemas.

Las herramientas de seguridad se clasificarán en base a su funcionalidad principal en las siguientes categorías:

a. Auditoría
b. Prevención
c. Detección
d. Respuesta

e. Conservación

Las herramientas de seguridad podrán operar a diferentes niveles (red, sistema, usuario, aplicación) o ser una combinación de todos ellos (multinivel).

a) **Herramientas de auditoría**. Son aquellas herramientas cuyo objetivo es el análisis del estado en materia de seguridad de los sistemas en un determinado momento. Entrarán en esta categoría herramientas como los escáneres de red, las de revisión de la configuración, las de auditoría de contraseñas y de código, las de análisis de metadatos y de vulnerabilidades.

b) **Herramientas de prevención**. Entrarán en esta categoría herramientas como los dispositivos de protección perimetral (*routers*, cortafuegos, *proxys*), de detección y prevención de intrusiones, de limpieza de metadatos, de gestión de contraseñas, los antivirus y filtros *anti spam*.

c) **Herramientas de detección**. Entrarán en esta categoría herramientas como las de captura, monitorización y análisis de tráfico de red, las de monitorización y supervisión de dispositivos de red, o las de monitorización y análisis de registros del sistema.

d) **Herramientas de Respuesta**. Entrarán en esta categoría herramientas como las de análisis de código dañino, las de gestión de incidencias.

e) **Herramientas de Conservación.** Entrarán en esta categoría herramientas como las de análisis forense y las de backup.

Cualquier herramienta de seguridad que pretenda incorporarse a los sistemas de información deberá ser previamente autorizada por el Responsable de

Seguridad de los Sistemas de Información, tras comprobar la idoneidad de la herramienta para el objetivo pretendido, su ajuste a los parámetros legales y de calidad y a los requisitos determinados en la presente norma.

Sin perjuicio de lo establecido en el apartado N/SEG/TEC-001-2, deberá existir un inventario y registro de las herramientas de seguridad en el que conste quiénes están autorizados para la instalación y desinstalación, configuración, modificación, mantenimiento y operación, así como el acceso a la información que, en su caso, pudiesen generar.

A la hora de aplicar cambios en la configuración de estas herramientas, requeridos por actualizaciones del proveedor, deberá tenerse en cuenta la necesidad o no de nuevas funcionalidades y, en cualquier caso, deberá acordarse con el Responsable de Seguridad de los Sistemas de Información la idoneidad del cambio en la configuración, ya que se debe a una situación creada por el proveedor y no por una necesidad del organismo y que, por tanto, no tiene por qué derivar en un cambio. En caso de que se realice el cambio, se deben documentar los requisitos de actualización y la motivación de la misma.

La operación de estas herramientas se ajustará a lo establecido en los procedimientos de operación del sistema que se citan al inicio de esta norma. No obstante, en cualquier caso, dichos procedimientos deberán abordar, como mínimo, los siguientes aspectos:

• Control de la configuración y gestión de la herramienta: Definiendo roles y perfiles a implementar, a fin de garantizar que los usuarios tienen el nivel de acceso adecuado a su labor y responsabilidad.

• Análisis y protección de datos: Se deberá indicar cómo manejar los datos que se obtengan a partir de la operación de la herramienta, así como las maneras de protegerlos frente a modificación, revelación, destrucción, etc. no autorizadas.

• Definición de operación básica, la cual debe cubrir la mayor parte del día a día de la operación de la herramienta.

• Gestión de incidentes derivados del uso de la herramienta, indicando las personas que deben ser informadas y que estarán identificadas en dichos procedimientos.

La documentación generada por las herramientas de seguridad deberá calificarse conforme a lo establecido en la norma N/SEG/USU-001-1, en cuya virtud se aplicarán las medidas pertinentes para su protección y distribución.

N/SEG/TEC-008 *SOFTWARE* DE GESTIÓN

N/SEG/TEC-008-1 INSTALACIÓN Y USO

Los usuarios no deberán instalar ningún tipo de *software*, ni siquiera copias del *software* propiedad de la corporación, por su propia iniciativa. Únicamente en casos debidamente justificados, y bajo las garantías de seguridad correspondientes, podrá autorizarse la instalación de determinado *software* por parte de los propios usuarios.

Cualquier necesidad de *software* o aplicación será canalizada a través del Servicio de Informática mediante el procedimiento habitual de peticiones de equipamientos y servicios, indicando también el fin de la petición. La petición, en

cualquier caso, deberá contar con la validación del máximo responsable técnico del Servicio o Unidad al que pertenezca el peticionario.

Toda solicitud será objeto del correspondiente análisis y valoración en el Servicio de Informática, con el fin de adecuarla a los recursos estándar de la Diputación de Valencia e implantar, en su caso, una alternativa óptima. La valoración deberá tener en cuenta los siguientes requisitos:

• Si existe un *software* con las mismas o similares características ya instalado en el entorno de la organización. No se producirán adquisiciones ni instalaciones de programas cuyas funcionalidades puedan ser similares a un *software* preexistente.

• Si el *software* solicitado es para tratar datos de carácter personal deberá proporcionar las garantías establecidas para este tipo de tratamientos. El producto especificará en su descripción técnica el nivel de seguridad que permite alcanzar.

• Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5] ENS.

• El *software* cumplirá las garantías recogidas en el apartado N/SEG/TEC-008-3.

N/SEG/TEC-008-2 DESARROLLO DE APLICACIONES

En el desarrollo de aplicaciones se cumplirán los siguientes requisitos:

- El desarrollo deberá realizarse sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción. El inventario de activos identificará expresamente los servidores utilizados para desarrollo.

- Se aplicará una metodología de desarrollo reconocida que tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida, trate específicamente los datos usados en pruebas y permita la inspección del código fuente.

- Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

- Formarán parte integral del diseño del sistema: Los mecanismos de identificación y autenticación; los mecanismos de protección de la información tratada y la generación y tratamiento de pistas de auditoría.
- Se aplicará una metodología de desarrollo seguro reconocida que:

    (a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
    (b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (overflow).
    (c) Tratará específicamente los datos usados en pruebas.
    (d) Permitirá la inspección del código fuente.

- Los siguientes elementos serán parte integral del diseño del sistema:
    (a) Los mecanismos de identificación y autenticación.
    (b) Los mecanismos de protección de la información tratada.

(c) La generación y tratamiento de pistas de auditoría.

- Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente y se anote su realización en el documento de seguridad si se afectan datos de carácter personal. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

N/SEG/TEC-008-3 ENTRADA EN PRODUCCIÓN

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se comprobará que se cumplen los criterios de aceptación en materia de seguridad y que no se deteriora la seguridad de otros componentes del servicio. Las pruebas se realizarán en un entorno aislado (pre-producción) y no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Cuando se trate de aplicaciones de sistemas de información de categoría MEDIA y superior, previamente a la entrada en servicio se realizará un análisis de vulnerabilidades que constará de tres fases:

- Revisión exhaustiva de los componentes del software, centrándose en su superficie de interacción con los usuarios con servicios de soporte y con otros programas.

- Análisis de posibles vulnerabilidades en los elementos identificados en el primer paso y estimación del impacto potencial que supondría un incidente.

- Pruebas de penetración para cerciorarse de si la vulnerabilidad es utilizable, priorizando aquellos puntos de mayor impacto potencial. Deben hacerse pruebas simulando usuarios externos y usuarios internos, en función de a quienes sea accesible el software.

Cuando se trate de aplicaciones de sistemas de información críticos o de categoría ALTA, además se realizará un análisis de coherencia en la integración en los procesos y se considerará la oportunidad de realizar una auditoría de código fuente. El análisis de coherencia abarcará los procesos administrativos implicados, realizando pruebas comprobando que los datos de entrada producen los datos de salida correctos, y que datos incorrectos de entrada son detectados y atajados antes de destruir la integridad del sistema.

N/SEG/TEC-009 SEGURIDAD EN ENTORNOS Y APLICACIONES *WEB*

La seguridad en el proceso de diseño y desarrollo de una aplicación *Web* debe abordar principalmente dos elementos:

a) El entorno de desarrollo *Web*, en el que se deberá disponer de la última versión que soluciona vulnerabilidades de seguridad previas y conocidas.
b) La aplicación *Web* propietaria, código propio, basada en el lenguaje de programación empleado.

Deberán consultarse de forma periódica las bases de datos de vulnerabilidades para estar al día sobre los últimos ataques, incidentes y vulnerabilidades sobre entornos *Web* y su impacto. Se recomiendan como fuentes de información detallada respecto a vulnerabilidades de seguridad CCN-CERT, *SecurityFocus* y SANS.

N/SEG/TEC-009-1 ESTRATEGIA Y METODOLOGÍA

Los elementos de seguridad principales de un entorno o aplicación *Web* deben incluir:

• Formación en seguridad de aplicaciones *Web*
• Arquitectura e infraestructura (sistemas y redes) segura
• Metodología de seguridad de desarrollo de aplicaciones *Web*
• Metodología de análisis de seguridad de aplicaciones *Web*

La estrategia y metodología de seguridad debe incluir adicionalmente los siguientes componentes:

• Formación en seguridad
• Instalación y configuración segura de sistemas y redes (arquitectura)
    - Actualizaciones: Servidor *Web* y de aplicación, *framework*, etc
• Desarrollo de *software* seguro
    - Gestión de versiones y actualizaciones
• *Web Application Firewalls* (WAF)
• Auditorías de seguridad
    - Caja negra: Pruebas de intrusión y *Web Application Security Scanners* (WASS)
    - Caja blanca: Revisión de código manual y automático
• Respuesta ante incidentes

N/SEG/TEC-009-2 ARQUITECTURAS DE SEGURIDAD EN ENTORNOS *WEB*

Se utilizarán preferentemente modelos de arquitectura de aplicaciones *Web* de tres capas (servidor *Web*, servidor de aplicación y base de datos).

La arquitectura de la aplicación *Web* debe disponer de mecanismos de detección y protección a nivel de red, incluyendo elementos de seguridad tradicionales como cortafuegos o sistemas de detección de intrusos.

Será necesario disponer de dispositivos dedicados exclusivamente a la inspección y filtrado del tráfico *Web*, es decir, el protocolo HTTP o HTTPS, ya que los cortafuegos tradicionales no disponen de capacidades avanzadas para analizar y bloquear los ataques recibidos a través de este protocolo.

En el caso de ser necesario asegurar la confidencialidad de las comunicaciones *Web* se hará uso de la versión segura del protocolo (HTTPS).

Adicionalmente a los elementos de seguridad propios de un entorno *Web*, es necesario proteger todos los elementos de la infraestructura en la que reside la aplicación *Web*, tales como dispositivos de comunicaciones (*routers, switches*, etc) o la infraestructura de servidores de nombres (DNS-SEC).

Los mecanismos de protección a implementar deben proteger los diferentes equipos frente a:

• Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno o aplicación *Web*.
• Ataques indirectos, donde cualquiera de los elementos es empleado como herramienta en el ataque.
• Ataques de denegación de servicio (DoS).

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de la aplicación *Web*: Software de los dispositivos de red y firewalls, sistema operativo de los servidores (*Web*, aplicación, y base de datos), y *software* de la plataforma de desarrollo empleada (PHP, ASP, Java, etc).

N/SEG/TEC-009-3 DESARROLLO SEGURO DEL *SOFTWARE* DE APLICACIONES *WEB*

El elemento fundamental en la metodología de seguridad de desarrollo de software de aplicaciones *Web* pasa por incluir todos los aspectos de seguridad en el ciclo de vida de desarrollo de *software* (SDLC, *Software Development Life Cycle*).

Se seguirán las especificaciones contenidas en la Guía CCN-STIC-812 en lo que respecta a las recomendaciones generales, filtrado de datos de entrada o acceso del usuario, gestión de mensajes de error, autentificación y gestión de sesiones, ataques CSRF, ataques de manipulación de URL, ataques de manipulación de información almacenada en disco, ataques a cookies, escalado de privilegios, y gestión de *Logs*.

N/SEG/TEC-009-4 ANÁLISIS DE SEGURIDAD DE APLICACIONES *WEB*

El objetivo del análisis de seguridad de una aplicación *Web* es pasar de una aplicación *Web* que presenta vulnerabilidades a una aplicación que es segura y no tiene vulnerabilidades conocidas. La metodología de análisis debe incluir dos áreas:

- Caja negra. El análisis de caja negra se centra en estudiar las vulnerabilidades de seguridad de la aplicación Web desde el punto de vista de un atacante externo.
- Caja blanca. El análisis de caja blanca se centra en estudiar las vulnerabilidades de seguridad de la aplicación Web desde el punto de vista del desarrollador.

La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

N/SEG/TEC-009-5 ADMINISTRACIÓN DE LA NAVEGACIÓN POR *INTERNET*

Para poder administrar la navegación por *internet* deberán establecerse los siguientes parámetros:

a) Los puertos autorizados. De forma que se predeterminen los diferentes puertos que se consideran autorizados para cada tipo de servicio (http; https; sftp…)

b) En su caso, los diferentes grupos de acceso (tipos de usuario de internet) en función de las categorías de páginas *web*.

c) El catálogo de tipos de fichero de acceso restringido, para minimizar los riesgos derivados de la descarga de ficheros.

d) La distribución de los distintos niveles de usuarios atendiendo a:

    - Las categorías de los contenidos para los que tienen permiso de acceso.
    - Los tipos de ficheros que tienen permiso de descarga.
    - Limitación del tiempo de consulta.

Los anteriores parámetros serán establecidos por el Comité de Seguridad TIC y documentados para su aplicación por los responsables de la administración de la navegación por *internet*.

Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.

N/SEG/TEC-010 SEGURIDAD EN ENTORNOS *CLOUD*

En este apartado se excluyen los posibles servicios de *Cloud Computing* que la Diputación de Valencia pudiese prestar a terceros, o para sí misma, mediante la utilización de activos internos (equipos, locales, personas, programas).

N/SEG/TEC-010-1 TIPOLOGÍA DE ENTORNOS *CLOUD*

A los exclusivos efectos de seguridad, se distinguirán los siguientes tipos de entornos *Cloud* externos -plataformas, programas o servicios que pueden ser utilizados por la Diputación como parte de los recursos (activos) para prestar un servicio y/o explotar una información-:

A) Entornos cuyos activos se encuentran bajo el control y gestión de la Diputación de Valencia. Se trata de plataformas, programas o servicios que se mantienen bajo su dominio de seguridad. Se aplican directamente las políticas y normas de seguridad internas.

B) Entornos cuyos activos se encuentran parcialmente bajo el control y gestión de la Diputación de Valencia. Normalmente por tratarse de servicios no integrales (IaaS, PaaS, CaaS, BaaS). Se aplicará lo previsto en el apartado N/SEG/TEC-010-3.

C) Entornos cuyos activos se encuentran bajo el control y gestión de un tercero. El tercero puede ser:

- Un ente público. Resulta indiferente si la puesta a disposición comporta algún tipo de contraprestación económica (tasa, etc) o no, si los recursos son de total propiedad del organismo público correspondiente o si se trata de una "puesta en común". Se aplicará lo previsto en el apartado N/SEG/TEC-001-3.
- Un ente privado. Normalmente proveedores de servicios *Cloud* de tipo generalista (Dropbox, Google Drive, Box, iCloud…) o bajo demanda; en este último caso, por resultar proveedores integrales (SaaS). Se aplicará lo previsto en el apartado N/SEG/TEC-010-3.

N/SEG/TEC-010-2 AUTORIZACIÓN PARA EL USO DE ENTORNOS *CLOUD*

La utilización de servicios *Cloud* requerirá en todos los casos la autorización del Comité de Seguridad TIC. La autorización podrá ser genérica, delimitando claramente los supuestos que se incluyen, sin margen de interpretación. La autorización deberá valorar los siguientes elementos:

a) Clasificación de la información implicada, según lo dispuesto en la norma N/SEG/USU-001-2
b) Normativa legal e interna de aplicación
c) Garantías de seguridad ofrecidas por el entorno
d) Análisis de riesgos
e) Alternativas técnicas o servicios similares
f) Opinión del Responsable de Seguridad de los Sistemas de Información

La autorización podrá quedar supeditada al cumplimiento de determinadas condiciones y/o la adopción de ciertas medidas, debiendo figurar todo ello en dicha autorización.

N/SEG/TEC-010-3 REQUISITOS DE SEGURIDAD

Los requisitos de seguridad que resulten de aplicación (N/SEG/TEC-001-1) no varían por el hecho de utilizar servicios *Cloud* externos. Pero los diferentes niveles de prestación del servicio (IaaS, PaaS, CaaS, BaaS, SaaS) y el modelo de despliegue (nube pública, privada o híbrida) condicionan las obligaciones de seguridad de las partes, por lo que deberá establecerse en un documento vinculante para el proveedor del servicio, con carácter general, sobre quién recaen dichas responsabilidades.

No obstante, dada la especialidad de este tipo de servicios, se seguirán siempre las siguientes indicaciones:

• Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC.

• Cuando se trate de servicios de simple alojamiento de información, y salvo que dicha información esté clasificada como PÚBLICA, todos los datos se cifrarán antes de salir del ámbito de la Diputación, de forma que los requisitos de seguridad sobre los proveedores se reducen a la dimensión de disponibilidad. El organismo será el único en poder de las claves de cifra, a las que aplicará lo previsto en el apartado N/SEG/TEC-014-2.

• En cualquier caso, las claves de cifra no se almacenarán en claro en la nube, ni se utilizarán en aplicaciones que se ejecuten en la nube.

• El proceso de autorización de usuarios (altas, bajas y gestión de derechos de acceso) no se realizará en la nube.

• Las aplicaciones de firma electrónica y de sellos de tiempo no se ejecutarán en proveedores de servicios *Cloud* de carácter general, sino con los medios propios o de terceras partes de confianza de acuerdo a la legislación aplicable en la materia.

• Los elementos virtualizados y los elementos de virtualización se tratarán igual que los elementos físicos correspondientes a efectos de configuración, mantenimiento, reglas de seguridad y aspectos regulatorios.

• Las imágenes de los elementos virtuales se tratarán como datos con los mismos requisitos de seguridad que la información y los servicios manejados por dichos elementos virtuales.

• Los componentes de seguridad del tipo DMZ, cortafuegos o agentes (proxy) no deberán residir en la misma máquina base que los componentes de producción.

• Se registrarán todas las actuaciones de creación, traslado, activación y destrucción de elementos virtuales. Asimismo, se registrará el montaje y la retirada de soportes de información, físicos o virtuales.

• Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría MEDIA según el Esquema Nacional de Seguridad.

• En el supuesto de sistemas de categoría MEDIA, además de lo anterior:

- No se compartirán equipos base con otras comunidades de usuarios.
- No se compartirá el mismo hipervisor con otras comunidades de usuarios.

- La administración del hipervisor estará separada de la administración de los elementos virtualizados: Diferentes interfaces, diferentes cuentas de administrador, y diferentes administradores.
- Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría ALTA según el Esquema Nacional de Seguridad.

• En el supuesto de sistemas de categoría ALTA, además de lo anterior:

- La red administrativa estará separada lógica (red privada virtual) o físicamente (red específica) de la red administrativa de otras comunidades de usuarios.

N/SEG/TEC-010-4 CONTRATACIÓN DE SERVICIOS *CLOUD*

Sin perjuicio de lo establecido en el apartado N/SEG/TEC-021-2, la contratación de servicios de *Cloud Computing* se llevará a cabo teniendo en cuenta lo siguiente:

• Los servicios en la nube se encuentran tipificados como contratos de servicio, de acuerdo con el artículo 10 del Real Decreto Legislativo 3/2011 por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público.

• Estos contratos deberán reflejar al menos los siguientes aspectos:

- Descripción del servicio
- Tipo de servicio (IaaS, PaaS, SaaS…).
- Tipo de infraestructura (nube pública, privada o híbrida).
- Capacidad del servicio.
- Protección de la información.

- Acuerdos de nivel de servicio (niveles, tiempos de respuesta, penalizaciones, etc.).
- Mecanismos de acceso al servicio.
- Responsabilidades y obligaciones
- Requisitos legales
- Requisitos para el cumplimiento del ENS
- Gestión de cambios
- Registro de actividad
- Gestión de incidentes
- Eliminación de información
- Respaldo y recuperación de datos
- Continuidad del servicio
- Finalización del servicio.
- Requisitos para la protección de datos personales

• Cuando el proveedor *Cloud* pueda contratar a un tercero como soporte de sus servicios (personal, instalaciones, servicios de comunicaciones, servicios de copias de respaldo…) estas subcontrataciones deberán estar previstas en el contrato, así como hacer constar que deben ser informadas y aceptadas por la Diputación de Valencia. Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor y de los servicios que de este último dependan; por tanto, deberá hacerse constar también en el contrato.

• Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información. Si el servicio en

la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

• El contrato podrá imponer condiciones sobre la ubicación geográfica de los servidores y/o de las líneas de comunicaciones en función de la información que vayan a acoger o a transportar respectivamente. Estas condiciones típicamente derivan de requisitos del propietario de la información como, por ejemplo, por razones horarias y de mayores facilidades para ejercer los controles y auditorías definidas, o de condicionantes legales respecto de la información (por ejemplo, en datos de carácter personal), permitiendo identificar el marco legal aplicable, garantizar en mayor medida su cumplimiento y reducir los riesgos asociados.

• El contrato definirá los roles de las personas involucradas en la prestación del servicio, tanto en la parte de la Diputación como del proveedor del servicio *Cloud*. Se deben considerar las siguientes responsabilidades mínimas. Al tratarse de procedimientos de coordinación, ambas partes deben definir a sus relativos interlocutores:

- Responsable de la seguridad
- Persona de contacto para incidentes de seguridad
- Persona de contacto para cambios y mantenimiento de sistemas
- Persona de contacto para incidencias relativas a los indicadores de servicio (SLA)
- Persona de contacto para aspectos contractuales
- Persona de contacto para temas jurídicos y regulatorios, en particular en lo relativo a datos de carácter personal

• Los requisitos de seguridad en estos contratos deben establecerse acordes con la Declaración de Aplicabilidad que corresponda y con el resultado del análisis

de riesgos, por lo que deberán ser previamente recabados del Responsable de Seguridad de los Sistemas de Información.

• Es necesario identificar en el contrato los derechos de la Diputación para poder monitorizar el funcionamiento del servicio y de este modo poder comprobar el cumplimiento de las medidas de seguridad, los controles y las políticas que garantizan la integridad, confidencialidad y disponibilidad de los datos, y del mismo modo poder realizar la comprobación de que el nivel de prestación es el pactado. La Diputación deberá reservarse siempre la potestad de auditoría respecto de los activos bajo el control y gestión del proveedor de servicios, incluidos los posibles subcontratistas, a efectos de comprobar de primera mano el cumplimiento de los requisitos contractuales.

• La finalización del servicio deberá estar recogida en la descripción del propio servicio, identificando la necesidad que pueda existir de que el proveedor devuelva la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto al tiempo que tardará el proveedor en realizar la migración de los datos. A este respecto se buscará la “neutralidad tecnológica” del servicio que facilite todo tipo de retorno o migración.

N/SEG/TEC-011 SEGURIDAD EN DISPOSITIVOS PORTÁTILES Y MÓVILES

Sin perjuicio de lo dispuesto en este apartado, se seguirá las pautas recogidas en las siguientes guías CCN para reforzar la seguridad de estos dispositivos:

· CCN-STIC-827 Gestión y uso de dispositivos móviles
· CCN-STIC-45X Seguridad de dispositivos móviles

Deberá elaborarse un procedimiento que contemple las directrices de puesta en operación, entrega y baja de los dispositivos portátiles y móviles.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

N/SEG/TEC-011-1 SEGURIDAD POR DEFECTO

La configuración de la seguridad por defecto a la que se refiere la norma N/SEG/USU-002-3 atenderá a los siguientes principios básicos:

• La limitación o restricción de la conexión directa a redes externas, de los canales, puertos y sistemas de comunicaciones de salida de información, de la instalación y ejecución de *software* y de los servicios que serán accedidos, será establecida por el Comité de Seguridad TIC atendiendo a los riesgos que para la seguridad estén presentes en función del tipo de dispositivo, el perfil de usuarios, la naturaleza de la información a tratar y el entorno de utilización.

• Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.

• Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

• Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos

imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

• Se evitará, en la medida de lo posible, que los dispositivos contengan claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

• En caso de que sea necesario almacenar claves en estos dispositivos, éstas estarán a su vez cifradas por otras claves que sólo el propietario del *hardware* que las tiene almacenadas sea capaz de generar y utilizar.

• Se implantarán soluciones de gestión centralizada de los dispositivos, del tipo MDM (*Mobile Device Manegement*) o similar, que permitan, en cualquier caso, la monitorización, el borrado remoto de datos o la realización de auditorías de seguridad sobre dichos dispositivos.

• Se procurará la entrega de los dispositivos con un filtro de privacidad integrado en el monitor o pantalla, de modo que se proteja de la visión de terceros.

• Para el cifrado de los dispositivos se recurrirá a las utilidades más indicadas, sean del propio sistema operativo, de la plataforma de gestión u otras soluciones específicas.

N/SEG/TEC-011-2 DISPOSITIVOS PORTÁTILES

Se preferirán los ordenadores portátiles en los que el acceso a la BIOS pueda estar protegida mediante un acceso con PIN/contraseña, únicamente conocido

por los configuradores de estos dispositivos del Servicio de Informática y Organización.

En todo caso, para los portátiles es aconsejable utilizar un sistema de cifrado en *pre-boot*, que pida una contraseña de acceso y descifrado del disco duro.

N/SEG/TEC-011-3 DISPOSITIVOS MÓVILES

Se preferirán sistemas operativos con menor incidencia contrastada de *malware*.

En el caso de sistemas operativos en los que sea factible que el usuario pueda disponer de los máximos privilegios administrativos sobre el dispositivo móvil y pueda tomar control completo del terminal (*jailbreak o rooting)*, las soluciones MDM adoptadas deberán contar con capacidades de detección para identificar si un dispositivo ha sufrido este tipo de procesos y notificar acerca de esta situación al administrador de seguridad.

Las soluciones MDM adoptadas dispondrán, en cualquier caso, de las siguientes funcionalidades de gestión:

- Restricciones de *software* y *hardware*
- Código de acceso
- Protección remota
- Gestión y borrado de datos remoto
- Servicios de localización
- Certificados digitales
- Comunicaciones (*wi-fi, Bluetooth*, etc)
- VPN
- Correo electrónico
- Navegación web

- APP's

En el caso de dispositivos aportados por los propios usuarios, si por cualquier razón técnica no pudiese garantizarse la seguridad o la incomunicabilidad entre el área profesional y la privada, de forma que quede salvaguardado el derecho a la privacidad, se denegará la posibilidad de uso del dispositivo en cuestión.

N/SEG/TEC-011-4 OTROS DISPOSITIVOS CONECTADOS A LA RED

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

a) Dispositivos multifunción: impresoras, escáneres, etc.
b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
c) Dispositivos internet de las cosas, en inglés Internet of Things (IoT).
d) Dispositivos de invitados y los personales de los propios empleados, en inglés Bring Your Own Device (BYOD).
e) Otros.

Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

N/SEG/TEC-012 FIRMA ELECTRÓNICA Y SELLADO DE TIEMPO

La utilización de firma electrónica requerirá de **una Política de Firma Electrónica y de Certificados**, aprobada por el órgano superior competente que corresponda, donde constará el conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas. Dicha Política deberá cumplir los requisitos del Esquema Nacional de Interoperabilidad.

Los sistemas podrán utilizar cualquier medio de firma electrónica de los reconocidos por la legislación vigente. En este sentido, los protocolos de firma electrónica harán uso de certificados digitales reconocidos. No se admitirá el uso de certificados cuya función resumen (*hash*) sea la función MD5 u otra de seguridad inferior.

Los sistemas de información de categoría MEDIA, además:

- Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

- Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación. El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

- Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

- Las firmas se protegerán con sellos de tiempo

Los sistemas de información críticos y los de categoría ALTA, además:

- Usarán dispositivos seguros de creación de firma
- Emplearán, preferentemente, productos certificados

Sin perjuicio de lo que pueda establecer la Política de Firma, en los sistemas de categoría ALTA habrá que cumplir con:

• Los sellos de tiempo prevendrán la posibilidad del repudio posterior.

• Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro. En todo caso, se fecharán electrónicamente los documentos cuya fecha y hora de entrada y/o de salida deba acreditarse fehacientemente.

• Se fecharán electrónicamente las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable; alternativamente se pueden utilizar formatos de firma avanzada que incluyan fechado.

• Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.

• Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.

• Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

• Se utilizarán productos certificados o servicios externos admitidos

• En los sistemas críticos y de categoría ALTA se hará uso de sistemas de sellado de tiempo que utilicen una Autoridad de Sellado de Tiempo (TSA) siendo de los denominados esquemas simples o esquemas enlazados.

N/SEG/TEC-013 SEGURIDAD DEL CORREO ELECTRÓNICO

N/SEG/TEC-013-1 HERRAMIENTA DE CORREO SEGURO

Deberá realizarse un análisis de los riesgos asociados al uso del correo electrónico, en base al cual se determinarán las condiciones que debe cumplir la herramienta utilizada para su gestión. Sin perjuicio de lo que resulte del citado análisis, deberán tenerse en cuenta los siguientes factores:

a) Cifrado. El sistema debe proporcionar cifrado robusto y basado en estándares internacionales.

b) Tránsito de datos. Si en la solución se produce tránsito de datos en texto claro, es necesario garantizar que dicho tránsito no afecta a la confidencialidad de la información corporativa y que se cumplen las restricciones legales de aplicación, en especial las relativas a datos de carácter personal.

c) Costes. La implantación de un sistema de correo seguro determinado puede suponer un cierto coste –tanto directo como indirecto-, por lo que es necesario analizar en términos económicos diferentes alternativas y aplicar la más adecuada en cada caso. El factor coste no debe anteponerse bajo ninguna condición al factor seguridad.

d) Facilidad de uso. La solución implantada debe ser sencilla en su uso diario, al menos de forma relativa.

e) Capacidad de integración. La solución a implantar debe integrarse todo lo posible tanto con las arquitecturas (red, *hardware*, *software*…) existentes en la organización como con el usuario, sus capacidades y sus necesidades.

f) Monitorización. La solución elegida, bien de forma directa bien a través de mecanismos indirectos, debe generar los registros correspondientes y disponer de capacidad de alerta ante situaciones anómalas que puedan repercutir en la seguridad de la información corporativa (intentos de acceso no autorizados, funcionamientos incorrectos, anomalías en el uso del sistema…)

N/SEG/TEC-013-2 SEGURIDAD DEL SERVIDOR DE CORREO

El servidor de correo electrónico corporativo deberá estar ubicado en una zona desmilitarizada (DMZ), y debe estar aislado tanto de Internet como de la red

interna de la organización mediante un cortafuegos correctamente configurado, que permita únicamente los tráficos estrictamente necesarios para el correcto funcionamiento de los sistemas y servicios corporativos.

En cualquier caso, el cortafuegos o los cortafuegos corporativos deberán controlar el tráfico que se permite hacia los sistemas de correo, tanto desde los equipos internos a la organización como desde los equipos ubicados en Internet.

Adicionalmente a las reglas anteriores, la Corporación, a través del Comité de Seguridad TIC, evaluará la conveniencia de denegar en el cortafuegos corporativo todo el tráfico SMTPs saliente hacia *Internet,* con excepción del generado en los servidores de correo electrónico, a fin de evitar, entre otros, propagaciones masivas de *malware* desde equipos de usuario, uso de equipos internos para realizar ataques de *phishing*, etc.

Al menos en los sistemas de categoría ALTA, deberán implantarse en la arquitectura sistemas de detección o prevención de intrusiones basados en red (NIDS/NIPS) que permitan identificar o incluso detener ataques o tráficos anómalos contra la plataforma de correo corporativo; los registros generados por estos entornos deben ser correctamente analizados para garantizar que se emprenden las acciones adecuadas ante una posible violación de la seguridad.

De la misma forma que el resto de sistemas corporativos, es crítico que los servidores de correo estén correctamente bastionados a nivel de sistema operativo. Para ello se seguirán las guías CCN-STIC correspondientes a cada sistema concreto, aplicando en éste las directrices que marcan dichos documentos.

El servidor o servidores de correo corporativo deben estar en sistemas dedicados, no compartiendo su funcionalidad con otros entornos de la

organización para evitar que vulnerabilidades en éstos afecten al correo electrónico. El *software* instalado en el servidor debe ser mínimo, eliminado aplicaciones no estrictamente necesarias para el funcionamiento del sistema de correo (herramientas ofimáticas, entornos de desarrollo, etc.).

En términos generales, deberán considerarse siempre los siguientes extremos:

a) Aplicación de parches y actualizaciones de seguridad en el sistema tan pronto como sea posible.

b) Eliminación de los servicios no necesarios para el funcionamiento correcto del sistema.

c) Restricciones de acceso adecuadas, tanto desde la red interna como desde *Internet*.

d) Políticas de gestión de usuarios y contraseñas robustas.

e) Permisos correctos en todo el sistema de archivos, prestando especial atención a las carpetas de correo de los usuarios.

f) Monitorización y control de parámetros que impliquen anomalías en la seguridad.

N/SEG/TEC-013-3 SEGURIDAD DE LOS SERVICIOS DE CORREO

Los servicios asociados al correo electrónico deben también configurarse de manera segura. Es especialmente importante garantizar, en primer lugar, que las versiones de las diferentes aplicaciones utilizadas para la gestión del correo en el servidor sean correctas tanto desde el punto de vista funcional como desde el punto de vista de seguridad, aplicando las actualizaciones proporcionadas por el

fabricante siempre que sea necesario. En segundo lugar, es necesario garantizar que la configuración de estas aplicaciones es correcta también desde ambos puntos de vista, ya que aplicaciones actualizadas convenientemente pero con una deficiente configuración son susceptibles de ser atacadas con éxito por un tercero.

Se debe limitar el acceso a los servicios de acceso al correo electrónico a aquellos orígenes desde los que efectivamente sea necesario acceder a la gestión de los mensajes por parte de los usuarios. En caso de que sea necesario el acceso a servicios de envío de correo desde *Internet*, deberá garantizarse en el tiempo que el servidor de correo no actúa como *open relay*, es decir, no permite ser utilizado para el envío de correo no deseado.

En el caso particular en que se requiera acceso *web* al correo corporativo, se debe garantizar la imposibilidad de acceder al entorno evitando la autenticación de éste. De la misma forma, debe garantizarse que los ataques vía *web* más habituales (XSS, SQL-i, LFI, RFI…) no afectan a la seguridad del servicio o aplicación *web*, bien mediante la implantación de sistemas de prevención de intrusiones que detecten y detengan los ataques antes de llegar al servidor, bien mediante un correcto bastionado del entorno *web* que proporciona correo electrónico a la organización. Independientemente de desde dónde esté permitido el acceso vía *web* al correo, el servidor *web* no debe estar ubicado en el propio MTA (Agente de Transferencia de correo, ubicado en el servidor) corporativo, sino en un servidor independiente a éste, y su bastionado y auditoría debe ser correcto y completo en el tiempo. Todas la comunicaciones entre el navegador –cliente- y el servidor *web* deben estar obligatoriamente cifradas, incluyendo en primer lugar la autenticación de usuarios.

N/SEG/TEC-013-4 SEGURIDAD DEL CLIENTE DE CORREO

Para garantizar la seguridad del correo electrónico corporativo, como elemento clave en el flujo de mensajes, es necesario garantizar la seguridad de los equipos de usuario utilizados para procesar dicho correo. Para ello, se debe bastionar el equipo de usuario de forma adecuada, sea cual sea su sistema operativo, teniendo en cuenta, sin menoscabo de otros cualesquiera, los elementos recogidos en las guías de seguridad para la configuración de servidores y de clientes de correo.

Los clientes de correo instalados en dichos equipos deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

N/SEG/TEC-013-5 SEGURIDAD DEL CONTENIDO

Cuando la información contenida en el cuerpo del mensaje deba protegerse de ataques de interceptación, deberá cifrarse convenientemente dicha información, bien mediante herramientas integradas en los clientes de correo, bien mediante herramientas independientes –adjuntando en este caso el archivo cifrado como un fichero más en el mensaje-. Siempre que sea posible se deben escoger herramientas integradas con los clientes de correo corporativos, de forma que se facilite al usuario la gestión segura de su correo desde el propio cliente de correo, sin necesidad de herramientas externas.

Pero cualquier sistema de seguridad en el correo electrónico debe incorporar no sólo el cifrado de la información, sino además la firma de ésta, sin importar su nivel de seguridad, de forma que el receptor por un lado descifre la información y, por otro, gracias a la firma digital, verifique que el receptor es quien dice ser y el contenido del correo es íntegro.

N/SEG/TEC-014 RECURSOS CRIPTOGRÁFICOS

N/SEG/TEC-014-1 USO DE CRIPTOGRAFÍA

Se llevará a cabo el cifrado de la información siempre que se trate de:

a) Aquella información cuya dimensión de confidencialidad sea valorada de nivel alto.

b) Los datos de carácter personal pertenecientes a las categorías especiales de datos. En estos casos deberá hacerse uso del mecanismo de encriptación incluso en las comunicaciones de datos realizadas en el ámbito interno de la propia organización (redes locales).

c) Aquella información que como resultado del análisis de riesgos así lo aconseje.

d) Cualesquiera otros supuestos recogidos expresamente en la normativa interna de seguridad y protección de datos personales.

En todos los casos se debe cifrar la información tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella. Esto incluye:

- Cifrado de ficheros
- Cifrado de directorios
- Discos virtuales cifrados
- Cifrado de datos en bases de datos

Para el cifrado de información, ya sea en tránsito o mientras esté almacenada, se utilizarán sistemas de cifrado seguros, siguiendo lo establecido en el apartado

N/SEG/TEC-006-2 para el cifrado de las comunicaciones. El Servicio de Informática aportará las soluciones técnicas necesarias para el cifrado de la información.

Cuando se reclamen productos certificados, se entenderá por tales todos aquellos que hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes de reconocida solvencia. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408, u otras de naturaleza y calidad análogas. Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad. Dado que la lista de los productos certificados es muy extensa y podría quedar obsoleta por la certificación de nuevos productos, se recomienda consultar las listas actualizadas de productos certificados de los organismos de acreditación y certificación anteriores.

Cuando se reclamen algoritmos o protocolos acreditados por el CCN se estará a lo indicado en el apartado N/SEG/TEC-014-2.

N/SEG/TEC-014-2 ALGORITMOS Y PROTOCOLOS ACREDITADOS

Se utlizarán los algoritmos y protocolos criptográficos que se consideran acreditados por el CCN para su uso dentro del Esquema Nacional de Seguridad, cuando sus características y requerimientos se consideren necesarios.

N/SEG/TEC-014-3 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

La protección de las claves de cifrado, independientemente de la seguridad que ofrezcan, cumplirá los siguientes requisitos:

• La protección abarcará todo el ciclo de vida de las claves: Su generación, transporte al punto de explotación, custodia durante la explotación, archivo posterior a su retirada de explotación activa y destrucción final.

• Se debe garantizar que las claves generadas son imprevisibles.

• Los medios de generación deben estar aislados de los medios de explotación. Las claves deben generarse en un equipo y después trasladarse al equipo en el que se van a usar. Los elementos de generación que no sean necesarios para el uso se quedarán en el equipo de generación. Es muy recomendable emplear un soporte de información (por ejemplo, un disco USB o una tarjeta de memoria) para trasladar las claves.

• En el transporte o distribución al punto de utilización, se debe asegurar la confidencialidad de la clave y la autenticidad del receptor. Si se opta por la entrega en mano, se utilizarán contenedores físicos seguros. En otro caso, se usarán contenedores criptográficos. Cabe la distribución por doble canal, clave y datos de activación por separado.

• Se utilizarán medios de generación y custodia en explotación evaluados o dispositivos criptográficos certificados. Dichos medios emplearán algoritmos acreditados por el CCN.

• Los medios de custodia en explotación deberán emplear tarjeta inteligente protegida por contraseña. Se debe procurar su cambio cuando el volumen de datos cifrados o el tiempo que lleva en uso superen los parámetros

recomendados antes de que un atacante pueda descubrirla por análisis de los datos cifrados.

• Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación (p.ej. en contenedores físicos seguros o en contenedores criptográficos). El Comité de Seguridad TIC determinará, cuando una clave se retire de explotación, durante cuánto tiempo se debe retener, bien por razones operativas, bien como prueba de auditoría. Es muy recomendable que las claves que se retienen estén en equipos separados. Para su uso se trasladará la información al equipo donde estén.

• Cuando deba procederse a la destrucción de claves se eliminará el original y todas sus copias. Se observará lo dispuesto en el apartado N/SEG/TEC-016-2.

• Existirá un registro que indique las actuaciones realizadas sobre cada clave en el sistema a lo largo de su ciclo de vida.

N/SEG/TEC-015 LIMPIEZA DE DOCUMENTOS

Deberá procederse a la limpieza de documentos electrónicos, de forma que se retire de ellos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento o resulte imprescindible para la correcta gestión de los documentos.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor *web* u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.
b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.
c) A la buena imagen de la organización que difunde el documento, por cuanto demuestra un descuido en su buen hacer.

Deberá existir un procedimiento para limpiar todos los documentos que van a ser transferidos a otro dominio de seguridad y para limpiar todos los documentos que van a ser publicados electrónicamente.

Se utilizarán herramientas evaluadas de análisis de meta-datos y para limpiar los datos ocultos innecesarios de los documentos, incluyendo los meta-datos existentes en ficheros adjuntos a correos electrónicos.

N/SEG/TEC-016 SOPORTES ELECTRÓNICOS

Los soportes electrónicos de información incluyen:

• Discos de los servidores y equipos de usuario final, con especial consideración a equipos móviles (portátiles y smartphones) y discos removibles
• PDAs
• Smartphones
• Disquetes, cintas, CD, DVD, ...
• Discos USB
• Tarjetas de memoria y tarjetas inteligentes
• Componentes de impresoras

• Otros medios electrónicos de almacenamiento de información con capacidad de que la información pueda ser recuperada de formar automática o manual

N/SEG/TEC-016-1 GESTIÓN DE SOPORTES

La gestión de los soportes de información se ajustará a lo dispuesto en la norma N/SEG/USU-002-4. Sin perjuicio de lo anterior, en el Servicio de Informática serán de aplicación, además, las siguientes directrices:

• Según el tipo de soporte, se aplicarán medidas contra su degradación o destrucción, y se determinarán los períodos de validez de los soportes atendiendo a la caducidad de los materiales utilizados en su fabricación.

• Los soportes que contengan información necesaria para garantizar la continuidad de los sistemas en caso de contingencia, deberán almacenarse alejados del equipo del que se ha extraído la información, en dispositivos que dificulten seriamente su exposición a agresiones de tipo físico o químico. Deberá conservarse un duplicado de dichos soportes en un establecimiento o local diferente al que se ubiquen los citados equipos.

• Los soportes que sean remitidos al Servicio de Informática para su borrado seguro y/o destrucción, deberán anotarse también en el registro de entradas y, en su caso, de salidas de soportes de dicho Servicio. Tras el borrado o destrucción se librará un documento de constancia del procedimiento llevado a cabo, el resultado y el estado final del soporte. Una copia del documento de constancia se hará llegar al remitente del soporte.

• Los soportes que, por cualquier tipo de avería o funcionamiento defectuoso, requiriesen de su traslado a locales de terceros deberán hacerlo sin albergar

ningún tipo de información, aplicándoles previamente un procedimiento de borrado seguro tal como se describe en el apartado N/SEG/TEC-016-2.

N/SEG/TEC-016-2 BORRADO SEGURO Y DESTRUCCIÓN

Los soportes que vayan a ser reutilizados para otra información, liberados a otra organización o destruidos serán objeto de un borrado seguro de su contenido. El método de eliminación de la información dependerá del nivel de sensibilidad de ésta:

a) Información clasificada como PÚBLICA. El borrado se efectuará mediante los comandos de borrado facilitados por la plataforma utilizada o utilidades generales, o a través de la recuperación del formato original del dispositivo.

b) Información clasificada como RESERVADA, RESTRINGIDA, CONFIDENCIAL y datos de carácter personal de categorías especiales. El borrado se efectuará mediante métodos de sobreescritura basada en datos, que garanticen el acceso a todas las áreas del soporte a borrar y que proporcionen pistas de auditoría del borrado. La sobreescritura de toda la información se realizará en tres fases: La primera con un valor, la segunda con el complemento a 1 del mismo, y la tercera con un valor aleatorio. Tras este proceso se debe verificar que toda la información se ha reescrito y que no han aparecido errores *hardware* en el procedimiento. Caso de aparecer errores se acudirá a la desmagnetización.

Cuando la naturaleza del soporte no permita el borrado seguro o cuando así lo requiera el procedimiento asociado a la información contenida, se destruirán de forma segura los soportes. La destrucción física de cualquier soporte electrónico de información deberá ir precedida de un proceso de borrado, que garantice la

imposibilidad de recuperación de cualquier tipo de dato mediante la transformación del medio en inservible. Se utilizarán para ello herramientas *hardware* del tipo desmagnetizador o similar, que estén certificadas conforme a lo establecido en el apartado N/SEG/TEC-021-3.

Se usarán productos o servicios que cumplan lo establecido en [op.pl.5] para el correcto borrado seguro y destrucción.

El procedimiento para el borrado seguro y destrucción de soportes de información contendrá las instrucciones precisas para el cumplimiento de la presente norma atendiendo a los diferentes tipos de soporte.

N/SEG/TEC-017 SEGURIDAD DE INSTALACIONES

Los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información se clasificarán en **Críticos (C)** y **No Críticos (NC)**.

Se calificarán como **Críticas** aquellas instalaciones que alberguen o contengan equipos que resulten estratégicos por su importancia en el funcionamiento regular de los sistemas de información, la seguridad de la información y el impacto en los servicios públicos.

N/SEG/TEC-017-1 CONDICIONES DE LAS INSTALACIONES

El equipamiento será instalado en áreas separadas específicas para su función. A estas áreas separadas solo se podrá acceder por las entradas previstas y vigiladas. Únicamente tendrán acceso al área las personas debidamente autorizadas. Se habilitarán dispositivos que impidan el acceso no autorizado. En

instalaciones No Críticas (NC), como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Los locales donde se ubiquen los sistemas de información y sus componentes deben contar con la potencia eléctrica necesaria. Se dispondrá de un análisis de la potencia eléctrica requerida, que se actualizará antes de la adquisición de nuevos componentes. Deberá contarse con las tomas eléctricas necesarias. De igual modo, se garantizará el correcto funcionamiento de las luces de emergencia, mediante la revisión periódica de las mismas. Será obligatorio en el caso de instalaciones Críticas (C) incorporar mecanismos que garanticen el suministro de potencia eléctrica en caso de fallo del suministro general (compuesto por SAI y, en caso de ser necesario, grupo electrógeno), de forma que se cuente con tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.

Los locales dispondrán de las adecuadas condiciones de temperatura y humedad, atendiendo a las especificaciones de los fabricantes de los equipos. Se instalarán mecanismos que permitan el control de los valores recomendados.

Los locales contarán con las protecciones adecuadas frente a las amenazas identificadas en el análisis de riesgos, tanto de índole natural como derivadas del entorno o con origen humano, accidental o deliberado. El cableado contará con la protección adecuada, mediante su etiquetado (para poder determinar las conexiones de cada cable físico), protección (para evitar tropiezos) y control (para evitar la existencia de cableado fuera de uso). Se dispondrá de un plano del cableado que incluya el etiquetado de los cables.

Se protegerán los locales frente a incendios, fortuitos o deliberados, conforme a la normativa industrial pertinente. Del mismo modo, se protegerán los locales frente a incidentes fortuitos o deliberados causados por el agua conforme al nivel

de riesgo identificado, lo que comporta la realización de un estudio de la ubicación física del local para conocer el riesgo real de problemas por causa natural o por el entorno.

N/SEG/TEC-017-2 USO DE LAS 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. Existirá un listado de las personas autorizadas.

El control de acceso a dichas áreas se efectuará mediante mecanismos que permitan identificar inequívocamente a la persona que accede, así como la fecha y hora de entrada y salida. Se llevará un registro en el que conste toda la información de acceso anterior. El registro será automatizado en caso de instalaciones Críticas (C). Cuando se trate de instalaciones No Críticas (NC) el registro podrá no estar automatizado, en cuyo caso deberá hacerse constar también la persona que efectúa el registro. Los datos del registro de accesos se mantendrán, como mínimo, durante un período de seis meses.

Cuando se realicen visitas autorizadas a dichas instalaciones, los visitantes deberán portar una identificación visible y estar acompañados en todo momento por la persona designada por el autorizante.

Está prohibida la existencia de material innecesario en el local, en particular material inflamable (papel, cajas, etc.) o que pueda ser causa de otros incidentes (fuentes de agua, plantas, etc.), y evitando que el propio local sea una amenaza o atraiga otras amenazas.

La permanencia en las salas se limitará al tiempo imprescindible para cumplir la tarea que justifica el acceso. Está prohibido comer, beber o practicar cualquier

actividad que pueda generar una amenaza para las instalaciones o los equipos que alberga. Cuando sean necesarias labores de mantenimiento o reparación que comporten el uso de agentes físicos o químicos agresivos (fuego, gas, herramientas, etc) deberán extremarse las precauciones y hacerse conforme a la normativa industrial y buenos usos profesionales.

Deberá mantenerse un registro pormenorizado de toda entrada y salida de equipamiento. El registro debe reflejar: Fecha y hora, identificación inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registro. Los datos del registro de entradas y salidas de equipamiento se mantendrán, como mínimo, durante un período de doce meses. El registro será llevado por el responsable del equipamiento, en tanto responsable de dichos activos del sistema.

N/SEG/TEC-017-3 INSTALACIONES ALTERNATIVAS

En caso de que las instalaciones habituales no se encuentren disponibles, cuando alberguen equipos de soporte a sistemas de categoría ALTA o por aconsejarlo el análisis de riesgos, deberá garantizarse la existencia y disponibilidad de instalaciones alternativas. Estas instalaciones alternativas deberán contar con idénticas garantías de seguridad que las instalaciones habituales.

N/SEG/TEC-018 INCIDENTES DE SEGURIDAD

N/SEG/TEC-018-1 CATEGORIZACIÓN DE INCIDENTES

Para su correcta gestión, todos los incidentes deberán estar clasificados. La clasificación de incidentes de seguridad dependerá de varios factores, como:

- La naturaleza del incidente
- La criticidad del/los sistema/s afectado/s
- El número de sistemas afectados
- El impacto que el incidente puede tener en la organización desde un punto de vista legal, de imagen pública, y de prestación de servicio
- Los requerimientos legales y regulatorios

Un incidente que contenga múltiples clases o tipologías debe ser clasificado por el evento de seguridad original o detectado inicialmente.

Se conformará la categorización de incidentes siguiendo las directrices de la guía CCN-STIC 817.

N/SEG/TEC-018-2 CRITERIOS PARA LA DETERMINACIÓN DE LA CRITICIDAD

Para poder dar el correcto seguimiento, determinar las prioridades y asignar recursos, es esencial que para cada incidente se determine qué nivel de criticidad se le asigna. Se emplearán una escala de criticidad con **5 niveles:**

A) Nivel de criticidad **BAJO**. Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC de la organización, pero que los controles de seguridad desplegados están

funcionando y contrarrestan adecuadamente la misma y por tanto su impacto es nulo o insignificante para la organización.

B) Nivel de criticidad **MEDIO**. Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC de la organización, y se sabe que ha tenido un impacto limitado en información considerada no crítica para la misión de la organización y/o sistemas TIC no críticos en la arquitectura de los sistemas TIC de la organización.

C) Nivel de criticidad **ALTO**. Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC de la organización, y se sabe que ha tenido un impacto considerable (afectación a la confidencialidad, disponibilidad o integridad) en información considerada no crítica para la misión de la organización y/o sistemas TIC no críticos en la arquitectura de los sistemas TIC de la organización.

D) Nivel de criticidad **MUY ALTO**. Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC de la organización, y se sabe que ha tenido un impacto considerable (afectación a la confidencialidad, disponibilidad o integridad) en información considerada crítica para la misión de la organización y/o sistemas TIC críticos en la arquitectura de los sistemas TIC de la organización.

E) Nivel de criticidad **CRÍTICO**. Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC de la

organización, y se sabe que ha tenido un impacto muy considerable (afectación total de la confidencialidad, disponibilidad o integridad) en información considerada crítica para la misión de la organización y/o sistemas TIC críticos en la arquitectura de los sistemas TIC de la organización.

N/SEG/TEC-018-3 GESTIÓN DE INCIDENTES

Se establecerá un procedimiento que contemple la gestión integral de los incidentes de seguridad: Comunicación, registro, tratamiento, respuesta y comunicación, en su caso, al CSIRT de ámbito autonómico.

Cuando se produzcan “alertas de seguridad” que deban ser comunicadas a los usuarios de los sistemas de información, éstas se canalizarán a través del Responsable de Seguridad de los Sistemas de Información.

N/SEG/TEC-018-4 GRUPO DE RESPUESTA A INCIDENTES TIC

En cumplimiento del artículo 15 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 deberá crearse un Grupo de Respuesta a Incidentes TIC (Grupo RITIC), cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de la Corporación. El Grupo RITIC estará formado por miembros designados por el Comité de Seguridad TIC.

Deberá elaborarse un procedimiento que establezca la forma de actuación del Grupo RITIC en caso de desastre.

N/SEG/TEC-019 ASISTENCIA REMOTA

Cuando se utilicen herramientas de asistencia técnica remota que impliquen el control remoto del ordenador o dispositivo del usuario, deberá recabarse previamente el consentimiento informado del usuario. Se intentará habilitar mecanismos automatizados que proporcionen la condición anterior y la constancia de ello. Las herramientas de asistencia remota deberán contar con registros de actividad que dejen evidencia de las acciones ejecutadas.

N/SEG/TEC-020 GARANTÍA DE CONTINUIDAD DE LOS SISTEMAS

N/SEG/TEC-020-1 COPIAS DE RESPALDO

Corresponde al Servicio de Informática la realización de copias de seguridad y recuperación de la información de todos los sistemas de información, así como del software que los trata, de modo que queden a salvo de cualquier contingencia que pueda conllevar su pérdida o comprometer su integridad.

Tal como se establece en la norma N/SEG/USU-001-6, en los casos en que se autorice la ubicación de la información en la propia estación de trabajo del usuario o en servidores o equipos no corporativos, el usuario será responsable de la integridad y copia de seguridad de la información y, por tanto, de su pérdida o modificación.

Las copias de seguridad deberán abarcar, como mínimo:

a) Información de trabajo de la organización.
b) Aplicaciones en explotación, incluyendo los sistemas operativos.

c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
d) Claves utilizadas para preservar la confidencialidad de la información.

La periodicidad de la copia de seguridad de cada información se fijará teniendo en cuenta los riesgos y lo crítica que sea la información, no pudiendo ser mayor a siete días el tiempo transcurrido desde que un dato es introducido en el sistema hasta que es salvado.

Deberá mantenerse un registro, si no lo produce automáticamente el propio software empleado en la realización de los *backup*, que permita conocer para cada información la fecha en que se realizó la última copia, la identificación del soporte físico en el que se realizó y la ubicación de almacenamiento del mismo.

Deberá elaborarse un procedimiento en el que se contengan los planes de realización de copias de seguridad y recuperación de los sistemas de información corporativos. Dichos planes recogerán los métodos, la periodicidad y las herramientas, así como la antigüedad de conservación de las copias. El procedimiento incluirá las actuaciones, el personal responsable y las autorizaciones, en su caso, que correspondan.

Cualquier modificación en el sistema que afecte a datos de carácter personal, como puede ser la implantación de nuevas aplicaciones, creación de nuevos ficheros, etc., deberá ser inmediatamente contemplado en el plan de recuperación, de modo que esta nueva información quede a salvo.

Las copias de seguridad poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según

proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Para garantizar la validez de los procedimientos de salvaguarda se deberán realizar comprobaciones de la integridad y consistencia de la información que contienen, y que las reservas son capaces de recuperar la información perdida ante la ocurrencia de un hipotético evento. Cuando se trate de datos de carácter personal, se deberá verificar semestralmente la fiabilidad de las copias de respaldo.

Para la recuperación de información de las copias de respaldo será necesaria la correspondiente autorización, en los términos recogidos en el apartado N/SEG/TEC-003.

La recuperación de datos se considerará un incidente de seguridad, debiendo anotarse en el registro indicado en la norma N/SEG/USU-006-2. El procedimiento de gestión de incidentes al que se refiere el apartado N/SEG/TEC-018-3 establecerá la información que deba anotarse en dicho registro.

Únicamente en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos de datos de carácter personal parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo de reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

Los soportes de copias de seguridad se ajustarán a lo establecido en el apartado N/SEG/TEC-016-1. Cuando se trate de datos de carácter personal de nivel ALTO, además:

• Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos.

• A las copias de datos almacenadas fuera del lugar de trabajo se les debe dar el mismo nivel de seguridad que a las que residan en las dependencias de la organización.

• Debe mantenerse un inventario del contenido que se encuentra en los lugares de almacenamiento externos.

N/SEG/TEC-020-2 ANÁLISIS DE IMPACTO

Aquellos sistemas cuya dimensión de disponibilidad sea de nivel MEDIO o ALTO deberán someterse a un análisis de impacto, es decir, a un estudio pormenorizado de cómo afectaría un desastre a la prestación de servicios, identificando los elementos del sistema de información que son necesarios para la prestación de cada servicio.

Deberá elaborarse un procedimiento con los criterios y pasos a seguir para la realización del análisis de impacto.

N/SEG/TEC-020-3 PLAN DE CONTINUIDAD

Deberá desarrollarse un Plan de Continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este Plan deberá contemplar obligatoriamente a todos los sistemas críticos y aquellos cuya dimensión de disponibilidad sea de nivel ALTO. El Plan será aprobado por el Comité de Seguridad TIC.

Este Plan contemplará los siguientes aspectos:

a) Se debe identificar funciones, responsabilidades y actividades a realizar en caso de desastre que impida prestar el servicio en las condiciones habituales y con los medios habituales. En particular:

   - Quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y avaluar las consecuencias.
   - Quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis.
   - Quiénes se encargan de reconstruir el sistema de información (recuperación de desastre).

b) Debe existir una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios en caso de no poder hacerse con los medios habituales:

   - Instalaciones alternativas.
   - Comunicaciones alternativas.
   - Equipamiento alternativo.
   - Personal alternativo.
   - Recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto.

c) El servicio alternativo ofrecerá las mismas garantías de seguridad que el servicio habitual. El plan debe determinar la coordinación de todos los elementos para alcanzar la restauración de los servicios en los plazos estipulados. Todos los medios alternativos deben estar planificados, y materializados en acuerdos o contratos con los proveedores correspondientes en su caso.

d) Las personas afectadas por el plan deben recibir formación específica relativa a su papel en dicho plan.

e) El plan de continuidad debe ser parte integral y armónica con los planes de continuidad de la organización en otras materias ajenas a la seguridad.

f) Deben establecerse procedimientos para sincronizar el plan de continuidad con las actualizaciones del sistema en lo referente a arquitectura, elementos componentes y servicios y calidad de los servicios prestados; es decir, los procedimientos operativos de seguridad referentes a cambios y actualizaciones deben incluir un punto para actualizar los planes de continuidad.

Se realizarán pruebas periódicas para localizar y corregir, en su caso, los errores o deficiencias que puedan existir en el plan de acción en caso de desastre.

Tras cada ejercicio debe realizarse un informe de análisis de las pruebas realizadas, destacando las incidencias propias o en proveedores externos y derivando un plan de mejoras, tanto en los medios como en los procedimientos y en la concienciación y formación de las personas implicadas.

N/SEG/TEC-021 CONTRATACIÓN

N/SEG/TEC-021-1 ADQUISICIÓN DE *HARDWARE* Y *SOFTWARE*

Para realizar la selección de equipos y paquetes de *software*, se evaluarán entre otros los siguientes aspectos:

• Facilidad y amigabilidad de uso.

• Mantenimiento sencillo del producto, que no implique costes adicionales.

• Compatibilidad e independencia de un *hardware* o *software* específico.

• Ciclo de vida de la instalación o *software*, con desarrollo de nuevas versiones de mejora o adaptación a cambios tecnológicos.

• Evitar, siempre que sea posible, *software* con protección de copias, que dificulte la recuperación del sistema en momentos de emergencia.

• El volumen de descuento por compras múltiples, y las condiciones de la licencia.

• La cobertura de asistencia técnica.

• Seguridad física y lógica.

El Servicio de Informática efectuará la selección de equipamiento y paquetes de *software*. Para ello, elaborará un análisis técnico de costes comparativo y enfocado a las necesidades del usuario final, valorando entre otros factores el precio del producto y los condicionantes (formación, instalación, mantenimiento, entrada de datos, etc.) que implica su puesta en funcionamiento.

Se considerarán especialmente como factores favorables para la adquisición de un producto o equipo la existencia en los contratos de compra o alquiler de cláusulas de mantenimiento, actualización de versiones, servicio de soporte técnico y formación en el producto.

Deberá establecerse un proceso formal para planificar la adquisición de nuevos componentes del sistema, que contemple lo previsto en esta norma y que además:

- Tenga en cuenta el análisis de riesgos.
- Se ajuste a la arquitectura de seguridad escogida.
- Prevea los recursos necesarios, esfuerzo y medios económicos para la implantación inicial, el mantenimiento a lo largo de su vida útil y la evolución de la tecnología.
- Atienda en todo momento tanto a las necesidades técnicas como a la necesaria concienciación y formación de las personas que van a trabajar con los componentes.

Todo ello sin perjuicio de lo establecido en el apartado N/SEG/TEC-007-2, en aquellos supuestos que resulte de aplicación.

N/SEG/TEC-021-2 CONTRATACIÓN DE SERVICIOS

Cuando se utilicen recursos externos a la Corporación, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones. La Corporación sigue siendo en todo momento responsable de los riesgos en que se incurre, en la medida en que impacten sobre la información manejada y los servicios finales prestados. Por ello se debe disponer las medidas necesarias para que la Diputación pueda ejercer su responsabilidad y mantener el control en todo momento, tal como se establece en el apartado N/SEG/TEC-001-3.

Con carácter general, cuando vaya a procederse a la contratación de servicios externos se tendrá en cuenta:

• Deben contratarse servicios que cuenten con la certificación de ENS conforme a la categoría del sistema dónde se implantará.

• Deben establecerse contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento (acuerdos de nivel de servicio).

• Resulta aconsejable realizar previamente un análisis de riesgos que identifique los riesgos asociados al proveedor externo.

• Si implica tratamiento de datos de carácter personal, se debe garantizar la aplicación de la normativa interna en la materia (N/PDP); debe considerarse especialmente:

- La existencia de encargado de tratamiento.
- Lugar de prestación de los servicios (locales de la Diputación o del proveedor).
- Exigencia de geolocalización.
- Cesiones de datos.
- Subcontratación.

• Las garantías de seguridad de la información, que quedarán detalladas en el documento contractual que resulte vinculante.

• Es recomendable recoger de forma agrupada las condiciones sobre confidencialidad, seguridad de la información y protección de datos de carácter personal; así como utilizar formatos de condiciones normalizados.

Cuando los servicios afecten a sistemas de categoría MEDIA y superior:

• Deberá realizarse un análisis de riesgos que identifique los riesgos asociados al proveedor externo.

• Deberá establecerse un contrato formal, aprobado por ambas partes y actualizado periódicamente, estableciendo:

- Roles y funciones de ambas partes en materia de seguridad, incluyendo los mecanismos de contacto.
- Obligaciones y responsabilidades de cada parte.
- Protocolo de aviso previo de actuaciones que puedan impactar a la otra parte.
- Mecanismos y procedimientos para la sincronización de las actividades de gestión de incidencias.

• Deberá establecerse un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado.

• Deberá establecerse el mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo, así como el mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.

N/SEG/TEC-021-3 ADQUISICIÓN DE PRODUCTOS Y SERVICIOS DE SEGURIDAD

En la adquisición de productos y servicios de seguridad de las TIC se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad

relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de Seguridad de los Sistemas de Información.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares reconocidos internacionalmente en el ámbito de la seguridad funcional. Tendrán la consideración de normas europeas o internacionales ISO/IEC 15408 u otras de naturaleza y calidad análogas.

En el caso de sistemas de categoría ALTA se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

La adquisición de las herramientas de seguridad descritas en el apartado N/SEG/TEC-007-5 se ajustará a las siguientes pautas:

• Los requisitos obligatorios de *hardware* y *software* de las herramientas de seguridad correspondientes deberán especificarse de manera detallada en los pliegos de prescripciones técnicas, los contratos para su adquisición o la propuesta vinculante.

• Los recursos adicionales que se consideren necesarios para la adecuada explotación de las herramientas de seguridad deben estar reflejados y tenidos en cuenta.

• En todo caso, se utilizarán preferentemente productos certificados cuando implementen las siguientes funcionalidades y mecanismos de seguridad:

- Mecanismo de autenticación

- Protección de claves criptográficas
- Protección de la confidencialidad
- Protección de la autenticidad y de la integridad
- Criptografía
- Borrado y destrucción
- Firma electrónica
- Sellos de tiempo

Las herramientas de cifrado software constituyen un grupo especial, que se regirá por lo dispuesto en el apartado N/SEG/TEC-014.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, en los términos recogidos en el apartado N/SEG/TEC-024 letra f).

Deberá exigirse, de manera objetiva y no discriminatoria, que las organizaciones que presten servicios de seguridad de los sistemas a la Corporación cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados y con profesionales cualificados.

Todas las herramientas y servicios de seguridad que se utilicen deberán ser previamente aprobados por el Responsable de Seguridad de los Sistemas de Información.

N/SEG/TEC-022 ANÁLISIS Y GESTIÓN DE RIESGOS

N/SEG/TEC-022-1 ASPECTOS BÁSICOS

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado. El análisis de riesgos debe permitir:

- Validar el conjunto de medidas de seguridad implantado
- Detectar la necesidad de medidas adicionales
- Justificar el uso de medidas de protección alternativas

Todo análisis de riesgos debe identificar y priorizar los riesgos más significativos a fin de conocer los riesgos a los que están sometidos los sistemas y tomar las medidas oportunas, técnicas o de otro tipo. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Sin perjuicio de otras referencias de ésta u otras normativas internas, que reclamen la necesidad de realizar un análisis de riesgos, deberá realizarse un análisis de riesgos:

a) Durante la especificación de un nuevo sistema, para determinar los requisitos de seguridad que deben incorporarse a la solución.
b) Durante el desarrollo de un nuevo sistema, para analizar opciones.
c) Durante la operación del sistema, para ajustar a nuevos activos, nuevas amenazas, nuevas vulnerabilidades y nuevas salvaguardas.

El riesgo residual debe estar documentado y aprobado por el responsable de la información y del servicio correspondiente(s). El Comité de Seguridad TIC determinará en cada momento el nivel de riesgo asumible por la organización para sus sistemas de información.

Deberá elaborarse un procedimiento para el análisis y gestión de riesgos. El procedimiento incluirá los criterios utilizados para seleccionar y valorar activos, amenazas y salvaguardas. Todo proceso de análisis de riesgos quedará documentado.

N/SEG/TEC-022-2 CRITERIOS Y METODOLOGÍA

La realización del análisis de riesgos estará en función de la categorización de cada sistema:

a) Sistemas de categoría BÁSICA o sin categorizar. El análisis de riesgos puede ser informal, es decir, llevado a cabo en un lenguaje natural en el que será suficiente identificar los siguientes aspectos:

   - Los activos más valiosos del sistema
   - Las amenazas más probables
   - Las salvaguardas que protegen de dichas amenazas
   - Los principales riesgos residuales

b) Sistemas de categoría MEDIA. Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

   - Identificación y valoración cualitativa de los activos más valiosos del sistema
   - Identificación y cuantificación de las amenazas más probables
   - Identificación y valoración de las salvaguardas que protegen de dichas amenazas
   - Identificación y valoración del riesgo residual

c) Sistemas críticos y de categoría ALTA. Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

- Identificación y valoración cualitativa de los activos más valiosos del sistema
- Identificación y cuantificación de las amenazas más probables
- Identificación de las vulnerabilidades habilitantes de dichas amenazas
- Identificación y valoración de las salvaguardas adecuadas
- Identificación y valoración del riesgo residual

Para los supuestos b) y c) se utilizará preferentemente MAGERIT, la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (Ministerio de Hacienda y Administraciones Públicas); siendo conveniente emplear alguna herramienta de soporte, tanto para la ejecución material como para afrontar la actualización regular de los cálculos ante nuevas amenazas o cambios en el sistema.

Todo ello conciliado con lo establecido en el apartado N/SEG/TEC-001-1.

N/SEG/TEC-023 AUDITORÍA DE LA SEGURIDAD

N/SEG/TEC-023-1 OBJETO Y TIPOS DE AUDITORIA

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.

   Además, el Delegado de Protección de Datos deberá de supervisar dichas auditorías, en virtud de lo establecido en el artículo 37 del citado Reglamento.

b) Auditorías, regulares o extraordinarias, en cumplimiento del RGPD y del Esquema Nacional de Seguridad. El objeto de estas auditorías de la seguridad, internas o externas, es el establecido en las normas N/SEG/USU-004-3 y N/SEG/USU-008. Son auditorías obligatorias y de carácter reglamentario.

N/SEG/TEC-023-2 AUDITORIAS DEL DEPARTAMENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

Las auditorías llevadas a cabo por el Departamento de Protección de Datos y Seguridad de la Información, y, en su caso, supervisadas por el Delegado de Protección de Datos, estarán determinadas en un procedimiento documentado que recogerá, como mínimo, las siguientes cuestiones:

- Objetivos de control
- Metodología

- Instrumentos o herramientas
- Periodicidad
- Informes

Los informes de resultados de las auditorías periódicas 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 a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de la Comunidad Autónoma.

N/SEG/TEC-023-3 AUDITORÍAS REGLAMENTARIAS

Las auditorías reglamentarias comprenden:

a) La verificación ordinaria (bienal) o extraordinaria (puntual) del cumplimiento de los requerimientos de seguridad establecidos por la normativa legal de aplicación y, en particular, por el Reglamento por el que se regula la Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia y su normativa de desarrollo.

b) La verificación ordinaria (bienal) o extraordinaria (puntual) del cumplimiento de las medidas de seguridad aplicables a los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de carácter personal.

Las auditorías reglamentarias se ajustarán a los siguientes requisitos:

• Por motivos de eficiencia y economía, estas auditorías se unificarán siempre que sea posible.

• Salvo en el supuesto a) del apartado N/SEG/TEC-023-4, el equipo auditor estará compuesto por profesionales de la auditoría de seguridad de sistemas de información, así como profesionales, en su caso, de la auditoría en protección de datos de carácter personal, todos ellos con experiencia contrastada y acreditaciones reconocidas (ISACA, ISC, APEP…).

• En la realización de las auditorías se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

• La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos sometidos a control.

• El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la normativa legal, la reglamentaria y la interna de la Corporación, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

• Los informes de auditoría serán analizados por el Responsable de Seguridad de los Sistemas de Información, que presentará sus conclusiones al Comité de Seguridad TIC para que adopte las medidas correctoras adecuadas.

• Los informes de resultados de las auditorías reglamentarias 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.

• Deberá elaborarse un procedimiento que recoja los requisitos y pautas de trabajo para la realización de las auditorías reglamentarias.

N/SEG/TEC-024 GESTIÓN DE LA SEGURIDAD

El Esquema Nacional de Seguridad exige la existencia un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección. El término gestión de la seguridad describe los procesos y actividades esenciales necesarias para el establecimiento y el mantenimiento del programa de seguridad de toda organización.

En el ámbito de la Diputación de Valencia la gestión de la seguridad de la información se rige por:

a) Principio de integridad. Tal como establece el artículo 11 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, la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, por lo que cualquier acción dirigida al objetivo de la seguridad debe considerar la interacción de todos los elementos citados, excluyendo cualquier actuación puntual o tratamiento coyuntural.

b) Análisis y gestión de riesgos. En aplicación del artículo 12 del citado Reglamento, la gestión de la seguridad se apoyará en un proceso continuo de análisis y tratamiento de riesgos. Este proceso deberá

mantenerse actualizado de modo permanente. A tal objeto, se seguirán las indicaciones del apartado N/SEG/TEC-022.

c) Monitorización de la seguridad. Es un proceso continuo que observa los sistemas e identifica los intentos de comprometer la seguridad de la organización. Para ello se atenderá especialmente a lo establecido en el apartado N/SEG/TEC-005-2.

d) Reevaluación periódica. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario. La aplicación de lo dispuesto en el apartado N/SEG/TEC-023 tiene dicha reevaluación como objetivo principal.

e) Mejora continua. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Toda estructura organizativa necesita una evaluación constante y un análisis de la respuesta a los incidentes de forma que se aprende de la experiencia, se corrigen defectos o debilidades y se busca la excelencia por medio de la mejora continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información. Deberá evaluarse el ciclo de madurez del sistema de gestión de la seguridad, criterios para la revisión y agenda de mejoras. Se aplicará a tal fin lo dispuesto en el apartado N/SEG/TEC-005-3.

f) Profesionalidad. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: Instalación, mantenimiento, gestión de incidentes y desmantelamiento. Tanto si se trata de personal interno como externo, la gestión de la seguridad corresponderá a profesionales con formación y experiencia contrastable sobre las materias concretas a tratar, que reúnan

las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. La independencia, en el caso de personal de seguridad interno, se ajustará a lo previsto en el artículo 16 del Esquema Nacional de Seguridad.

Toda la documentación generada por la aplicación de los elementos anteriormente citados forma parte del sistema de gestión de la seguridad de la información. Con carácter anual, el Responsable de Seguridad de los Sistemas de Información preparará un informe que recoja una síntesis de dicha documentación y las conclusiones más relevantes, del cual dará traslado al Comité de Seguridad TIC para que determine las posibles actuaciones que considere oportunas, a la vista de dichas conclusiones.

N/SEG/TEC-025 MARCO DE RESPONSABILIDADES

La responsabilidad del Responsable de Seguridad de los Sistemas de Información a la que se refiere el artículo 29 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 limitada a la ejecución de los cometidos de determinar las medidas de seguridad que han de ser implantadas y de supervisar su correcta implantación.

La responsabilidad del Responsable de los Sistemas de Información TIC y, en su caso, de los Responsables del Sistema delegados, consiste en cerciorarse de que las medidas específicas de seguridad determinadas por el Responsable de Seguridad se integren adecuadamente en cada Sistema de Información TIC dentro del marco general de seguridad.

La responsabilidad del Administrador de Seguridad de los Sistemas de Información TIC y, en su caso, de los Administradores de Seguridad delegados, se circunscribe a la implantación, gestión y mantenimiento de las medidas de seguridad determinadas por el Responsable de Seguridad aplicables a cada Sistema de Información TIC.

La responsabilidad del Departamento de Protección de Datos y Seguridad de la Información comprende la supervisión del cumplimiento de los requisitos legales y de la normativa interna en materia de seguridad de la información, en el marco 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.

Cuando, en la ejecución de su labor de supervisión, el Responsable de Seguridad de los Sistemas de Información constate el incumplimiento o inobservancia de cualquier medida de seguridad deberá comunicarlo a quien considere responsable de su subsanación. Estos hechos se considerarán incidentes de seguridad y serán tratados conforme a lo dispuesto en el apartado N/SEG/TEC-018-3.

N/SEG/TEC-026 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.