MUNICIPIOS

Ayuntamiento de Cortes de Pallás

2025/12239 *Anuncio del Ayuntamiento de Cortes de Pallás sobre la aprobación definitiva del Reglamento Regulador de de la Política de Seguridad y Normativa de Seguridad.*

ANUNCIO

El Ayuntamiento Pleno, en sesión celebrada el día 31/07/2025, aprobó inicialmente el Reglamento Regulador de la Política de Seguridad y la Normativa de Seguridad como cumplimento de Esquema Nacional de Seguridad. Sometido el acuerdo al trámite de información pública y no habiéndose presentado alegaciones dentro del plazo establecido, por la Alcaldía se ha dictado Resolución nº 752 de fecha 07/10/2025, elevando a definitivo dicho acuerdo, cuyo texto íntegro se hace público para su general conocimiento y en cumplimiento de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local.

Contra el presente acuerdo, se podrá interponer recurso contencioso-administrativo ante la Sala Contencioso Administrativo del Tribunal Superior de Justicia de la Comunidad Valenciana en el plazo de dos meses a contar desde el día siguiente a la publicación del presente anuncio, de conformidad con el artículo 46 de la Ley 29/1988, de 13 de Julio, de la Jurisdicción Contencioso-Administrativa.

VER ANEXO

Cortes de Pallás, 13 de octubre de 2025.—El alcalde, David Gras Arlandis.

Documento1: POLITICA DE SEGURIDAD DEL ENS:

POLÍTICA DE SEGURIDAD

ESQUEMA NACIONAL DE SEGURIDAD

D. DAVID GRAS ARLANDIS, mayor de edad, con DNI 53722464F, actuando en nombre y representación del AYUNTAMIENTO CORTES DE PALLAS, provisto de CIF P4610100B, y con domicilio a efectos de notificaciones en PLAZA DE LA IGLESIA, Nº 14, 46199 - Cortes de Pallás (Valencia/València).

Esta Normativa General de Seguridad de la información es efectiva desde la fecha de aprobación 02/07/2025, y hasta que esta sea reemplazada por una nueva Política de seguridad.

IDENTIFICACIÓN CONTACTO:

Denominación social: AYUNTAMIENTO CORTES DE PALLAS

CIF/NIF: P4610100B

Actividad: Otras actividades

Teléfono de contacto: 962336005

Domicilio social: PZ IGLESIA, Nº 14, 46199 - Cortes de Pallas (Valencia/València)

Domicilio a efecto de notificaciones: PZ IGLESIA, Nº 14, 46199 - Cortes de Pallas (Valencia/València)

Dirección electrónica de contacto: informatica@cortesdepallas.es

Página web (URL): www.cortesdepallas.es

1.- OBJETO

AYUNTAMIENTO CORTES DE PALLAS (en adelante, la entidad) depende de los sistemas TIC (Tecnología de Información y Comunicaciones) para alcanzar sus objetivos.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS en adelante), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

2.- ALCANCE

La presente política de seguridad ha sido desarrollada e implementada bajo la normativa exigida. Esta política se aplica a todos los sistemas TIC recogidos en el documento, que forma parte de su sistema generado para documentar las medidas mínimas de seguridad exigidas por el ENS, bajo la denominación “Declaración de Alcance”.

3.- LEGISLACIÓN Y NORMATIVA APLICABLE

Ley 34/ 2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Ley 39/2015 de 1 de octubre, de administrativo común de las administraciones públicas.

Ley 40/2015 de 1 de octubre, de régimen jurídico del sector público.

Ley Orgánica 3/ 2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la ley de propiedad intelectual.

Real Decreto 203/ 2021, de 30 de marzo, por el que se aprueba el reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016.

GUÍAS CCN-STIC.

UNE - ISO/IEC 27002:2013 código de buenas prácticas para la gestión de la seguridad de la información.

UNE - ISO/IEC 27001:2013 especificaciones para los sistemas de gestión de la seguridad de la información.

UNE-EN-ISO 9001:2015 sistemas de gestión de la calidad.

4.- VIGENCIA

La presente Política de Seguridad ha sido aprobada por la dirección de la entidad, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la entidad pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la entidad.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Política de Seguridad.

5.- PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de activos de información.

La entidad depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos.

Dichos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando a los incidentes.

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos: a) Seguridad como proceso integral. b) Gestión de la seguridad basada en los riesgos. c) Prevención, detección, respuesta y conservación. d) Existencia de líneas de defensa. e) Vigilancia continua. f) Reevaluación periódica. g) Diferenciación de responsabilidades.

De este modo, las amenazas no se materializarán y en caso de que ocurriese la idea principal es que no afecten gravemente a la información que maneja, o los servicios que se prestan.

Se desarrollarán, al menos los siguientes objetivos:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

5.1.- PREVENCIÓN

La entidad debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello los departamentos o áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.2.- Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el artículo 10 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

“La vigilancia continua permitirá la detección de actividades o comportamiento anómalos y su oportuna respuesta. 2.La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. 3.Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.”

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

“El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita: a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto. b) Minimizar el impacto final sobre el mismo. 2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.”

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.3.- Respuesta

Los departamentos o áreas deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

5.4.- Recuperación

Para garantizar la disponibilidad de los servicios críticos de la entidad deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

6.- ORGANIZACIÓN DE LA SEGURIDAD

6.1.- Definición de roles

La implantación de la Política de Seguridad en la entidad requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos de seguridad, requisitos del sistema y requisitos del servicio.

Es por ello por lo que, la Política de Seguridad, según se detalla en el ANEXO II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su sección 3.1, deberá identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros.

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección será responsable de organizar las funciones y responsabilidades, la política del Organismo, y por último de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

6.2.- Comité de Seguridad: Funciones y Responsabilidades

La seguridad de la Información es una responsabilidad organizativa. En consecuencia, se promueve la composición de un Comité de Seguridad de la Información, con el interés de establecer una vía definida y de apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por cada una de las figuras, que en este epígrafe se detallan, de responsables y por un presidente que será responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.
    - Elaboración y actualización de planes de continuidad.
    - Cumplimiento y difusión de las Políticas de Seguridad.

Para documentar la composición del Comité de Seguridad se utiliza el documento adjunto a la presente Política de seguridad como ANEXO I

6.3.- Roles y Responsabilidades

Los diferentes roles de seguridad de la información se limitan a una jerarquía simple: el Comité de Seguridad de la Información y los diferentes Responsables, donde rige el principio básico de diferenciación de responsabilidades tal y como se establece en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Diferenciando así el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

Por su parte, el Delegado de Protección de Datos debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad.

En concreto, la organización debe designar los siguientes roles:

RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información de la entidad establecerá los requisitos, en materia de seguridad, de la información gestionada.

Se deberá tener en cuenta que, si dicha información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la normativa de protección de datos.

Las obligaciones del Responsable de la Información son:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer en los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información en la entidad.

Se ha designado como Responsable de la Información a la persona recogida en el documento adjunto a la presente Política como ANEXO II.

Se adjunta en la presente Política como ANEXO IV comunicado formal para la designación de Responsables de la Información, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLE DEL SISTEMA

El Responsable del Sistema asegurará la ejecución de medidas para protección de los activos y de los servicios de los sistemas de información que soportan la actividad de la entidad.

Las obligaciones del Responsable del Sistema son:

- Desarrollar, operar y mantener el Sistema de Información la entidad durante el ciclo de vida, especificaciones, instalación y verificación de su correcto funcionamiento.

- Cerciorarse de que las medidas específicas de seguridad de la entidad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de la entidad conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en la entidad.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. o Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

Se ha designado como Responsable del Sistema a la persona recogida en el documento adjunto a la presente Política como ANEXO II.

Se adjunta en la presente Política como ANEXO VI comunicado formal para la designación del Responsable de Seguridad, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLE DE SEGURIDAD

El Responsable de la Seguridad de la Información de la entidad será el responsable de la coordinación y verificación de cumplimiento de los requisitos de seguridad de la información.

Las obligaciones del Responsable de la Seguridad son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Coordinar la realización de un análisis de riesgos, así como implantar los controles necesarios para reducir los riesgos.

- Reportar al Delegado de Protección de Datos sobre violaciones de seguridad de los datos personales.
- Difundir las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de la entidad.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Supervisar y velar por el cumplimiento de la normativa legal aplicable.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad acaecidos en la entidad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Se ha designado como Responsable de Seguridad a la persona recogida en el documento adjunto a la presente Política como ANEXO II.

Se adjunta en la presente Política como ANEXO V comunicado formal para la designación del Responsable de Seguridad, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLES DEL SERVICIO

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado.

Las obligaciones del Responsable del Servicio son:

- Velar por el uso que se haga de determinados servicios y de la protección de estos.

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Gestionar los tratamientos de datos personales, en cuanto al Reglamento 2016/ 679 General de Protección de Datos, por delegación del Responsable del Tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión del tratamiento de datos personales que se realizan en su área.

Se ha designado como Responsable/s de Servicio a la/s persona/s recogida/s en el documento adjunto a la presente Política como ANEXO II.

Se adjunta en la presente Política como ANEXO III comunicado formal para la designación de Responsables de Servicio, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

6.4.- Difusión, actualización y revisión de la política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

La Política será aprobada por el Órgano de Gobierno y esta será difundida para que la conozcan todas las partes afectadas.

La normativa de seguridad deberá estar a disposición de todos los miembros de la entidad.

Será el Responsable de Seguridad la persona encargada de la custodia y difusión de la versión aprobada de la documentación generada.

7.- DATOS DE CARÁCTER PERSONAL

La entidad trata datos de carácter personal. La política de Protección de Datos y las Medidas de Seguridad al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables de tratamiento correspondientes.

Todos los sistemas de información de la entidad se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las actividades de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará de este modo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

8.- GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política de Seguridad de la Información deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por la normativa, según lo previsto en el artículo 7 del ENS.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo autónomo, a través de un Plan de Adecuación al ENS.

Este análisis se repetirá:

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

El análisis de riesgos también contemplará los requisitos establecidos por el artículo 32 del RGPD para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

9.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la entidad en diferentes materias:

- (La entidad debe hacer una lista de referencias a otras políticas en materia de seguridad e insertarlas en este apartado).

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros la entidad que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

- La política de seguridad se encuentra disponible en las instalaciones de la organización.

10.- OBLIGACIONES DEL PERSONAL

Todos los miembros de la entidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros atendrán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Las sesiones de concienciación deberán quedar registradas mediante la cumplimentación del Anexo de la presente Política REGISTRO DE ACCIONES FORMATIVAS VII.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la entidad, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11.- TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la entidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. La entidad ha aprobado un procedimiento específico recogido en el documento PROCEDIMIENTO DE REPORTE DE INCIDENTES DE SEGURIDAD.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12.- REFERENCIAS

La entidad debe incluir en este apartado todas las referencias documentales y legislativas que apoyan o completan esta Política de seguridad, o que se hayan tenido en cuenta a la hora de redactarla. Añadir tantos apartados como sea necesario.

REGISTRO DE NOMBRAMIENTO MIEMBROS DEL COMITÉ DE SEGURIDAD

FECHA APROBACIÓN	**julio de 2025**
PRESIDENTE	**ALCALDE**
VICEPRESIDENTA	**RESPONSABLE DE SEGURIDAD**
SECRETARIA	**SECRETARIA DEL AYUNTAMIENTO**
VOCALES	**RESPONSABLES DE SERVICIO**

ANEXO I

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA
DE SEGURIDAD DEL ESQUEMA NACIONAL DE SEGURIDAD

Mediante la cumplimentación de la presente declaración, el abajo firmante, como usuario del sistema de información **AYUNTAMIENTO CORTES DE PALLAS**, dice haber leído y comprendido la Política de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

Siendo las principales funciones de este Comité de Seguridad las siguientes:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.
    - Elaboración y actualización de planes de continuidad.
    - Cumplimiento y difusión de las Políticas de Seguridad.

En _____, a ____ de _____ de 20__

Denominación de la entidad:	
NIF de la entidad:	
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario:	

Por la entidad:

D./ Dña. _____
DNI número: _____

ANEXO II

NOMBRAMIENTO DE ROLES

RESPONSABLE DE LA INFORMACIÓN:

RESPONSABLE DE LA SEGURIDAD:

RESPONSABLE DEL SISTEMA:

RESPONSABLES DEL SERVICIO:

RESPONSABLES DEL SERVICIO	SERVICIO

ANEXO III

NOMBRAMIENTO DE RESPONSABLES DEL SERVICIO ANEXO III

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DEL ENS COMO RESPONSABLE DEL SERVICIO

Mediante la cumplimentación de la presente declaración, el abajo firmante, como Responsable del Servicio del sistema de información AYUNTAMIENTO CORTES DE PALLAS, dice haber leído y comprendido la Política de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

Siendo las principales obligaciones del Responsable del Servicio las siguientes:

- Velar por el uso que se haga de determinados servicios y de la protección de estos.
- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Gestionar los tratamientos de datos personales, en cuanto al Reglamento 2016/ 679 General de Protección de Datos, por delegación del Responsable del Tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión del tratamiento de datos personales que se realizan en su área.

En CORTES DE PALLÁS, julio de 2025

Denominación de la entidad:	AYUNTAMIENTO DE CORTES DE PALLÁS
NIF de la entidad:	P4610100B
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario: *(Firmado electrónicamente al margen)*	

Por la entidad: AYUNTAMIENTO DE CORTES DE PALLÁS

Dña.
DNI número:

ANEXO IV

NOMBRAMIENTO DE RESPONSABLE DE LA INFORMACIÓN ANEXO IV

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DEL ENS COMO RESPONSABLE DE LA INFORMACIÓN

Mediante la cumplimentación de la presente declaración, el abajo firmante, como Responsable de la Información del sistema de información AYUNTAMIENTO CORTES DE PALLAS, dice haber leído y comprendido la Política de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

Las obligaciones del Responsable de la Información son:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. (Materia de protección de datos)
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

En CORTES DE PALLÁS, julio de 2025

Denominación de la entidad:	AYUNTAMIENTO DE CORTES DE PALLÁS
NIF de la entidad:	P4610100B
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario: *(Firmado electrónicamente al margen)*	

Por la entidad: AYUNTAMIENTO DE CORTES DE PALLÁS

D.
DNI número:

ANEXO V

NOMBRAMIENTO DE RESPONSABLE DE SEGURIDAD ANEXO V

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA
DE SEGURIDAD DEL ENS COMO RESPONSABLE DE SEGURIDAD

Mediante la cumplimentación de la presente declaración, el abajo firmante, como Responsable de Seguridad del sistema de información AYUNTAMIENTO CORTES DE PALLAS, dice haber leído y comprendido la Política de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

Las obligaciones del Responsable de la Seguridad son:

- Mantener el nivel adecuado de seguridad de la información y realizar o promover las auditorías periódicas a las que obliga el ENS.
- Coordinar la realización de un análisis de riesgos e implantar los controles para reducir los riesgos.
- Reportar al Delegado de Protección de Datos sobre violaciones de seguridad de los datos personales.
- Difundir las normas y procedimientos contenidos en la Política de Seguridad.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Supervisar y velar por el cumplimiento de la normativa legal aplicable.
- Comprobar que las medidas de seguridad existente son las adecuadas.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad acaecidos desde su notificación hasta su resolución, emitiendo informes sobre los más relevantes al Comité.

En CORTES DE PALLÁS, julio de 2025

Denominación de la entidad:	AYUNTAMIENTO DE CORTES DE PALLÁS
NIF de la entidad:	P4610100B
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario: *(Firmado electrónicamente al margen)*	

Por la entidad: AYUNTAMIENTO DE CORTES DE PALLÁS

Dña.
DNI número:

ANEXO VI

NOMBRAMIENTO DE RESPONSABLE DEL SISTEMA ANEXO VI

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA POLÍTICA
DE SEGURIDAD DEL ENS COMO RESPONSABLE DEL SISTEMA

Mediante la cumplimentación de la presente declaración, el abajo firmante, como Responsable del Sistema del sistema de información AYUNTAMIENTO CORTES DE PALLAS, dice haber leído y comprendido la Política de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

Las obligaciones del Responsable del Sistema son:

- Desarrollar, operar y mantener el Sistema de Información durante el ciclo de vida, especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. o Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

En CORTES DE PALLÁS, julio de 2025

Denominación de la entidad:	AYUNTAMIENTO DE CORTES DE PALLÁS
NIF de la entidad:	P4610100B
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario: *(Firmado electrónicamente al margen)*	

Por la entidad: AYUNTAMIENTO DE CORTES DE PALLÁS
D.
DNI número:

ANEXO VII

REGISTRO DE ACCIONES FORMATIVAS VII

La entidad se rige, entre otros, por el principio de información y formación, según el cual una de las claves para garantizar la seguridad de la información es la formación e información que se facilite al personal involucrado en el tratamiento de la misma, educando a los empleados en la denominada cultura de la seguridad de la información.

En su consecuencia, todo el personal de la entidad con acceso a información será convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la Política de seguridad, recibiendo el apropiado conocimiento, capacitación y actualizaciones regulares de la seguridad de la información.

En relación con la metodología de las acciones informativas y formativas, se recomienda la combinación de diferentes metodologías para una mejor asimilación de los conocimientos por parte de los participantes, citando a modo de ejemplo las siguientes:

- Exposición de contenidos o clase magistral: El docente explica los contenidos de forma teórica con ayuda de recursos como son presentaciones de PowerPoint.
- Simulaciones o estudio del caso: El docente propone situaciones a resolver por parte de los participantes, que le permiten asimilar mejor los conocimientos adquiridos.
- Dinámicas de grupo: Con el fin de activar la interacción entre los participantes y el docente.

Con la finalidad de la gestión de control interno del cumplimiento del principio de información y formación en el seno de la entidad, se ha elaborado un “Registro de acciones formativas e informativas” para el personal en materia de seguridad de la información.

Documento 2: NORMATIVA DE SEGURIDAD DEL ENS:

1.- OBJETO

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), este documento contiene la Normativa General de Seguridad de AYUNTAMIENTO CORTES DE PALLAS (en adelante, la entidad), gestionados o bajo la responsabilidad de la entidad, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a la entidad, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la entidad:

- Facilitar y agilizar la tramitación de nuestros servicios, mediante el uso de herramientas informáticas y aplicaciones de gestión.
- Proporcionar información completa, homogénea, actualizada y fiable.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la entidad determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Por tanto, la presente Normativa General de Seguridad, tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

Este documento se considera de uso interno y, por consiguiente, no podrá ser divulgado salvo autorización expresa de la entidad.

2.- ALCANCE

La presente normativa de seguridad ha sido desarrollada e implementada bajo la normativa exigida. Esta política se aplica a todos los sistemas TIC recogidos en el documento, que forma parte de su sistema generado para documentar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, bajo la denominación “Alcance”.

3.- LEGISLACIÓN Y NORMATIVA APLICABLE (identico al Documento Politica de Seguridad).

4.- VIGENCIA

La presente Normativa General de Seguridad de ha sido aprobada por Comité de Seguridad de la entidad, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la entidad pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa General de Seguridad.

5.- REVISIÓN Y APROBACIÓN DE LA NORMATIVA GENERAL DE SEGURIDAD

La gestión de esta Normativa General de Seguridad corresponde al Responsable de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente, o con menor periodicidad si existen circunstancias que así lo aconsejen, el Responsable de Seguridad revisará la presente Normativa General de Seguridad.

La revisión se centrará en la actualización de las novedades legislativas que se hubieran producido en el último periodo revisado, la identificación de oportunidades de mejora en la gestión de la seguridad de la información, infraestructura tecnológica, organización sistemas de información, etc.

Cuando el Responsable de Seguridad, como resultado de la revisión, estime necesario realizar modificaciones en la presente Normativa propondrá al Comité de Seguridad la aprobación del texto definitivo.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

6.- UTILIZACIÓN DE EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES

La entidad facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la entidad pone a disposición de los usuarios deben utilizarse para el desarrollo de fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

6.1.- Normas Generales

- Los equipos informáticos serán asignados por el Responsable de Seguridad de acuerdo con lo establecido en el documento “Procedimiento de gestión de soportes” que forma parte de la estructura documental del ENS.

En cualquier caso, existirá un inventario actualizado de todos aquellos recursos físicos (hardware) que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos, siguiendo el esquema incluido en el ANEXO II adjunto.

- A cada nuevo usuario que se incorpore a la organización, el Responsable de Seguridad, o en su defecto el Responsable de servicio designado, facilitará el “MANUAL DE RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS” que recoge las siguientes normas de uso:

- Equipo informático
- Correo electrónico
- Carpetas departamentales
- Credenciales de acceso a los sistemas de información
- Dispositivos móviles
- Soportes informáticos

- Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Únicamente el personal autorizado por el Responsable de Seguridad podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Responsable de Seguridad. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa del Responsable de Seguridad, los usuarios no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta al Responsable de Seguridad de tales circunstancias.
- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
- Los usuarios deberán notificar al Responsable de Seguridad, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.
- En todo caso el usuario será informado por el Responsable de Seguridad sobre cómo reportar incidentes de seguridad mediante el documento “Procedimiento de reporte de incidentes”.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet.

- Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Responsable de Seguridad, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones de la entidad estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

6.2.- Usos específicamente prohibidos

Los usuarios de los sistemas de información tienen totalmente prohibidos los siguientes comportamientos:

- Se prohíbe el uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, para el tratamiento de datos de carácter personal responsabilidad la entidad, salvo que medie autorización expresa y previa adopción de las medidas de seguridad adecuadas al riesgo.
- Está totalmente prohibido el uso, total o parcial, de información para un uso particular o de terceros, con o sin ánimo lucrativo. Toda información generada como resultado del desarrollo de funciones laborales encomendadas es propiedad de la entidad.
- Utilización de cualquier tipo de software no autorizado.
- Utilización de programas que hagan un uso abusivo de la red.
- Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.).
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la entidad, sin la previa autorización del Responsable de Seguridad.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por el Responsable de Seguridad.

- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa del Responsable de Seguridad.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente.

6.3.- Normas específicas para el almacenamiento de información

Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios será objeto de salvaguarda mediante procedimiento corporativo de copia de seguridad.

La entidad puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria. En cualquier caso, todos los usuarios de los sistemas de información seguirán las instrucciones facilitadas por el Responsable de seguridad en relación al almacenamiento de información.

No está permitido, salvo autorización expresa al efecto, el uso de dispositivos de almacenamiento inalámbricos.

No está permitida información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa la entidad.

6.4.- Normas específicas para equipos portátiles y móviles

Cuando los empleados utilicen dispositivos móviles propiedad de la entidad para el desarrollo de las funciones encomendadas, se deberán cumplir las siguientes normas:

- El uso de dispositivos móviles propiedad de la entidad estará restringido a los fines estrictamente relacionados con el desempeño de las labores encomendadas al empleado.
- Se prohíbe a los usuarios poseedores de un dispositivo móvil propiedad de la entidad la cesión, préstamo o venta del mismo a otras entidades, independientemente de que éstas pertenezcan o no a la Organización.
- Se prohíbe la alteración, por parte del usuario, de las características del dispositivo móvil que puedan suponer una reducción del nivel de seguridad del mismo. Así mismo se prohíbe la instalación de cualquier tipo de software en el dispositivo móvil sin autorización.

- Es responsabilidad de los usuarios hacer uso de los dispositivos móviles con las máximas garantías de seguridad y desde emplazamientos seguros de forma que se minimicen los riesgos, impidiéndose el acceso por parte de entidades no autorizadas a estos dispositivos.
- Los usuarios nunca deberán dejar los dispositivos móviles desatendidos, o en lugares en los que se pueda poner en riesgo tanto el propio dispositivo móvil como la información contenida o que pueda ser accedida a través de él.
- En caso de pérdida o robo del dispositivo móvil, se deberá comunicar el incidente de seguridad a través de los procedimientos y cauces establecidos.

6.5.- Normas específicas para pendrives

Con carácter general, el uso de memorias USB no está autorizado. En su caso, la autorización deberá proporcionarla el Responsable de Seguridad.

Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y Responsable de Seguridad.

En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por la entidad que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario, no debiendo ser usados fuera de éstos.

Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. El Responsable de Seguridad podrá poner a disposición de los unidades de almacenamiento en red, que podrán usarse para tal propósito.

La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Responsable de Seguridad, de forma inmediata.

6.6.- Grabación CD´s y DVD´s

Con carácter general, el uso de equipos grabadores de CD´s y DVD´s no está autorizado. En su caso, la autorización deberá proporcionarla el Responsable de Seguridad.

Por razones de seguridad, los equipos grabadores de CD´s y DVD´s de los puestos de trabajo estarán deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del Responsable de Seguridad.

6.7.- Copias de Seguridad

Mantener copias de seguridad es una cautela esencial de protección de la información.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente.

Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en una unidad de red compartida.

De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas donde se almacene la información del usuario. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

6.8.- Borrado y eliminación de soportes informáticos

Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

- Asegurarse del contenido de cualquier soporte antes de su eliminación.
- Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por la entidad.

Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por la entidad, previa petición del Responsable de servicio.

El proceso para llevar a cabo el borrado de cualquier activo se encuentra recogido en el documento “Procedimiento de gestión de soportes” aprobado por la entidad.

6.9.- Impresoras en red, fotocopiadoras y fax

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

En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la entidad y, en su consecuencia, estén debidamente inventariados.

Los usuarios de los sistemas de información deberán respetar la Política de uso de impresoras aprobada por la entidad:

- Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

- Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente
- Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.

6.10.- Digitalización de documentos

Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida. Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente.

6.11.- Cuidado y protección de la documentación impresa

Los usuarios de los sistemas de información deberán respetar la Política de mesas limpias:

- La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.
- Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de forma que no sea recuperable la información que pudieran contener.
- Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.
- Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

6.12.- Pizarras y Flipcharts 45

Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiaran adecuadamente las pizarras y flipcharts de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

6.13.- Protección de la Propiedad Intelectual

Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la entidad sin la correspondiente licencia de uso.

Los programas informáticos o licenciados están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa de la entidad.

Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización de la entidad.

6.14.- Protección de la dignidad de las personas

Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

7.- INSTALACIÓN DE SOFTWARE

Únicamente el personal de soporte técnico autorizado por la entidad podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

Excepción a esta norma serán aquellas herramientas de uso común incluidas en el ANEXO III de la presente normativa (CATALOGO DE APLICACIONES AUTORIZADAS) descargables desde los servidores internos a la entidad.

Todo usuario podrá solicitar la inclusión de una aplicación en dicho CATALOGO DE APLICACIONES AUTORIZADAS para su estudio.

El proceso para llevar a cabo la instalación de cualquier software se encuentra recogido en el documento “Procedimiento de gestión de soportes” aprobado por la entidad.

No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.

Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la entidad de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas, especialmente aquellas relacionadas con la seguridad.

8.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

Los datos gestionados y tratados por cualquier Sistema de Información de la entidad deben tener asignado un responsable (Responsable del servicio), que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

Para el alta de nuevos usuarios se aplicará el proceso aprobado por la entidad en el documento “Procedimiento de gestión de soportes”. La autorización para acceder a los sistemas de información (ANEXO IV) establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos para la realización de sus funciones.

Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por la entidad en caso de un grave incumplimiento del usuario de las distintas normativas y procedimientos internos aprobados por la entidad.

Cuando un usuario deje temporalmente su puesto de trabajo resulta necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 5 minutos.

La baja de los usuarios será comunicada al Responsable de Seguridad, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo, en los términos previstos en el “Procedimiento de gestión de soportes.”

9.-IDENTIFICACIÓN Y AUTENTIFICACIÓN

Los usuarios dispondrán de un código de usuario (user-id) y una contraseña (password) o bien una tarjeta criptográfica con certificado digital, para el acceso a los Sistemas de Información de la entidad, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso y deberá registrarse en el ANEXO V (al que únicamente tendrá acceso el Responsable del sistema).

Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Responsable de Seguridad la correspondiente incidencia de seguridad.

El procedimiento para la creación y utilización de contraseñas robustas está descrito en la Política de «Buenas prácticas en la gestión de contraseñas» en relación con el acceso a los datos personales responsabilidad de la entidad y a los equipos utilizados para su tratamiento. A tal fin, se han seguido las orientaciones y directrices recogidas en los siguientes documentos:

- Guía de Seguridad de las TIC. CCN-STIC 821. Apéndice V: Normas de Creación y Uso de Contraseñas NP40. Centro Criptológico Nacional (CCN).
- Políticas de seguridad para la pyme: contraseñas. Instituto Nacional de Ciberseguridad (INCIBE).
- Recomendaciones de la Agencia Española de Protección de Datos (AEPD).

10.- ACCESO Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS DE LA ENTIDAD

Los terceros ajenos a la entidad que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- El personal ajeno que temporalmente deba acceder a los Sistemas de Información de la entidad deberá hacerlo siempre con autorización (ANEXO VI) y bajo la supervisión de algún miembro acreditado y previa autorización del Responsable de Seguridad.
- Para los accesos de terceros a los sistemas de información, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.
- Los usuarios autorizados, en lo que les sea de aplicación, deberán cumplir puntualmente la presente Normativa General de Seguridad, así como el resto de normativa de seguridad especialmente en lo referente a los apartados de salida y confidencialidad de la información.
- Para acceder a los edificios, instalaciones o dependencias de la entidad deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse al personal de Control de

Acceso y solicitar la presencia de la persona responsable de la entidad que constituirá su enlace durante su estancia en él.

- La acreditación personal que se le proporcione en el Control de Acceso deberá portarse en lugar visible en todo momento, debiendo ser entregada a la salida.
- Una vez en el interior de los edificios, dependencias o instalaciones de la entidad, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aseos, comedor, zona de máquinas de cafetería, etc.).
- Asimismo, deberán tener autorización del enlace cuando tengan necesidad de realizar desplazamientos entre distintos departamentos de la entidad.
- Los terceros atendrán siempre los requerimientos que le hiciere el personal de control y seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.
- Cualquier incidencia que surja antes o en el transcurso del acceso a los sistemas de información deberá ponerlo en conocimiento de su enlace. La función del enlace será dar asesoramiento, atender consultas o necesidades, transmitir instrucciones, ponerle al corriente de sus cometidos, objetivos, etc.

11.- CONFIDENCIALIDAD DE LA INFORMACIÓN

Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por la entidad (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella una absoluta reserva por tiempo indefinido.

Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.

Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.

La información contenida en los Sistemas de Información es propiedad de la entidad, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa del Responsable de Seguridad.

Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador.

Como medida de protección de la información está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada por el Responsable de Seguridad.

12.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y CONFIDENCIALIDAD

La Dirección / Órgano de Gobierno de la entidad asume la máxima responsabilidad y compromiso con el establecimiento, implementación y mantenimiento de la presente Política de Protección de Datos, garantizando la mejora continua del responsable del tratamiento con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y de la normativa española de protección de datos de carácter personal (Ley Orgánica, legislación sectorial específica y sus normas de desarrollo).

En su consecuencia, la entidad apuesta por una política proactiva de cumplimiento en pos de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

Así, ex art. 32.4 RGPD, el responsable del tratamiento deberá tomar las medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable.

De otro lado, a finales del año 2018 fue aprobada en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD). Dicha Ley Orgánica adapta el ordenamiento jurídico español al modelo establecido en el Reglamento general de protección de datos, introduciendo nuevos aspectos mediante el desarrollo de materias contenidas en el mismo.

En tal sentido, la citada LOPDGDD recoge un artículo específico relativo al deber de confidencialidad, señalando lo siguiente:

“Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento”.

En consecuencia, los usuarios del sistema de información deben cumplir con las normas de seguridad que se recogen en el documento “MANUAL DE RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS.

13.- TRATAMIETNO DE LA INFOMACIÓN

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

Cualquier tratamiento en los Sistemas de Información deberá ser conforme con la legislación vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos. Así mismo, los usuarios de los sistemas de información deberán respetar y cumplir todas las normativas, procesos y políticas internas que han sido aprobadas por la entidad y puestas a su disposición.

14.- SALIDAS DE INFORMACIÓN

La salida de información (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por el Responsable de Seguridad (ANEXO VII).

La salida de datos sensibles, confidenciales, o protegidos requerirá su cifrado previo o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

Los usuarios se abstendrán de sacar al exterior cualquier información de la entidad en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos debidamente autorizados.

15.- COPIAS DE SEGURIDAD

Si un usuario está autorizado para almacenar información en forma local (por ejemplo, en el disco duro del PC asignado), deberá tener en cuenta que es responsable de realizar las copias de seguridad de la misma. Por este motivo, se recomienda que los usuarios almacenen sus ficheros de trabajo en las carpetas de red habilitadas al efecto.

Por parte del Responsable de seguridad, se realizarán 5 copias de seguridad semanales, una por día, de los ficheros del sistema de almacenamiento en red (carpetas del servidor) y del resto de sistemas corporativos.

16.- CONEXIÓN DE DISPOSITIVOS A LA REDES DE COMUNCIACIONES

No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por el Responsable de Seguridad, salvo autorización previa de la entidad.

17.- USO DEL CORREO ELECTRÓNICO CORPORATIVO

Los empleados requieren del uso del correo electrónico para el desarrollo de sus funciones. Se considera correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, de Internet.

La entidad pone a disposición de sus empleados una cuenta de correo electrónico corporativa para que puedan desarrollar adecuadamente las tareas que tienen encomendadas.

En el ámbito del uso del correo electrónico, los empleados, así como los colaboradores externos, deberán cumplir las siguientes normas:

- La cuenta de correo corporativa únicamente podrá ser utilizada para finalidades directamente relacionadas con el desarrollo de las funciones laborales.
- Los usuarios son responsables de todas las actividades realizadas con sus cuentas de correo corporativas.
- El usuario cuidará en todo momento el lenguaje utilizado en sus comunicaciones por correo electrónico, debiendo tener presente que en cada una de ellas compromete la imagen y el nombre de la entidad.
- No se deben enviar correos de forma masiva sin justificación adecuada.
- Los usuarios han de ser precavidos en cuanto a los correos recibidos, especialmente si éstos provienen del exterior. Por ello no se deben abrir o responder a correos electrónicos de fuentes no confiables y de dudosa procedencia, así como abrir o ejecutar cualquier tipo de fichero adjunto procedentes de dichas fuentes.
- No se enviarán sin autorización correos electrónicos que contengan datos de carácter personal a personas que no pertenezcan a la Organización.
- La transmisión de datos de carácter personal a través de redes de telecomunicaciones y en particular a través de correo electrónico se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

En relación al uso del correo electrónico, las siguientes actividades están expresamente prohibidas:

- Utilizar una cuenta de correo electrónico que no sea la corporativa para el desarrollo de las funciones laborales encomendadas.

- Utilizar el correo electrónico corporativo con fines comerciales ni lucrativos para su beneficio.

- Suplantar la identidad de otra persona en el envío de mensajes de correo electrónico.

- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin su consentimiento, con el fin de descubrir sus secretos o vulnerar su intimidad, bien apoderándose o bien interceptando sus comunicaciones o utilizando artificios técnicos de escucha, grabación o reproducción del sonido, la imagen o cualquier otra señal de comunicación.

- Facilitar los datos necesarios para el uso de la cuenta de usuario y buzón a otras personas.

- Utilizar la cuenta de correo corporativo para participar en foros o grupos de noticias donde se expresen opiniones personales. El correo electrónico está ligado a la imagen pública de la entidad.

- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios (spam).

- Enviar o reenviar indebidamente mensajes en cadena o de tipo piramidal.

- El envío de mensajes o imágenes con contenido ilegal, ofensivo, difamatorio o inapropiado, o discriminatorios por razones de género, raza, edad, sexo, discapacidad, u ofensivos de cualquier forma así como aquellos que promuevan el acoso sexual.

- La falsificación de las cabeceras de correo electrónico.

18.- ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

El acceso corporativo a Internet es un recurso centralizado que la entidad pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

La entidad velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

18.1.- Normas Generales

- Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos.
- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la entidad en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del Responsable de seguridad.
- Deberá notificarse al Responsable de seguridad cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

18.2.- Usos especialmente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de programas informáticos sin la autorización previa del Responsable de seguridad o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por el Responsable de Seguridad.

18.3.- Incidencias de Seguridad

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la entidad o su imagen, deberá actuar inmediatamente de acuerdo con el proceso definido en el documento “Procedimiento de reporte de incidentes”.

En todo caso, el responsable de seguridad documentará la existencia de incidentes de seguridad mediante el Libro registro al efecto incluido en el Anexo VIII.

19.- COMPROMISO DE LOS USUARIOS

Los usuarios de los sistemas de información conocerán el contenido de la presente normativa, a tal fin, suscribirán el recibí adjunto como ANEXO I.

Los Usuarios de los Sistemas de Información deberán suscribir, o al menos conocer, el compromiso de confidencialidad incluido en el documento MANUAL DE RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS.

20.- INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de entidad están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información y Sistema de información.

El incumplimiento de las normas de uso del sistema de información establecidas en el presente documento podrá tener como consecuencia la imposición de las sanciones disciplinarias correspondientes, sin perjuicio del ejercicio de las acciones laborales, civiles o penales que, en su caso, procedan y las responsabilidades que de dicho ejercicio se deriven.

21.- ACCESIBILIDAD

Todos los usuarios de los recursos informáticos y/o Sistemas de Información deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa General de Seguridad de la Información.

ANEXO I

ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DEL ESQUEMA NACIONAL DE SEGURIDAD

Mediante la cumplimentación de la presente declaración, el abajo firmante, como usuario del sistema de información de AYUNTAMIENTO CORTES DE PALLAS, dice haber leído y comprendido la Normativa de Seguridad del Esquema Nacional de Seguridad de la misma y se compromete, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Denominación de la entidad:	
NIF de la entidad:	
Nombre y apellidos del usuario:	
DNI del usuario:	
Firma del usuario:	

Por la entidad:

D./ Dña. _____
DNI número: _____

ANEXO II

INVENTARIO DE ACTIVOS DE INFORMACIÓN (El inventario de activos deberá seguir esta estructura mínima, pudiendo utilizar cualquier software para su desarrollo, siendo recomendable el uso de formato Excel**)**

Usuario/ Propiedad del activo	NºReferencia/ Host	Marca/ Fabricante	Modelo/ Procesador	MAC	IP	Software instalado	Tipo de activo	Fecha de creación	Fecha de destrucción	Área local/ departamento	Tipo de datos que contienen

ANEXO III

CATÁLOGO DE APLICACIONES AUTORIZADAS

APLICACIÓN	DESCRIPCIÓN	FECHA DE ALTA	FECHA DE BAJA

ANEXO IV

AUTORIZACIÓN ACCESO A LOS SISTEMAS DE INFORMACIÓN Y DATOS PERSONALES TRATADOS

Autorizaciones y Habilitaciones				
Horario de trabajo:				
Ubicación del puesto de trabajo:				
Áreas con acceso físico autorizado				
		SÍ	NO	Observaciones
Planta 0	Zona 1			
	Zona 2			
	Zona 3			
Planta 1	Zona 1			
	Zona 2			
	Zona 3			
Uso de teléfono:				
Uso del puesto de trabajo:				
Uso ordenador portátil:				
Conexión a la red corporativa:				
Salida a Internet:				
Servidores con acceso autorizado	Tipo 1			
	Tipo 2			
	Tipo 3			
Acceso a control de versiones:				
Acceso a gestor documental:				
Acceso a carpetas de red:				
Otras:				

ANEXO V

IDENTIFICACIÓN USUARIOS Y CONTRASEÑAS (Este documento únicamente será accesible para el Responsable de sistema)

IDENTIFICACIÓN	USUARIO	CONTRASEÑA

ANEXO VI

Autorizaciones y Habilitaciones				
Horario de trabajo:				
Ubicación del puesto de trabajo:				
Áreas con acceso físico autorizado				
		SÍ	NO	Observaciones
	Zona 1			
Planta 0	Zona 2			
	Zona 3			
Planta 1	Zona 1			
	Zona 2			
	Zona 3			
Uso de teléfono:				
Uso del puesto de trabajo:				
Uso ordenador portátil:				
Conexión a la red corporativa:				
Salida a Internet:				
Servidores con acceso autorizado	Tipo 1			
	Tipo 2			
	Tipo 3			
Acceso a control de versiones:				
Acceso a gestor documental:				
Acceso a carpetas de red:				
Otras:				