NORMATIVA DE USO DE LOS SISTEMAS

Ayuntamiento de Martos

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de uso de los sistemas		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-001 Normativa de uso de los sistemas.docx		
Clasificación:	Uso Interno		
Estado:	Documento		
Autor:	Consultor Externo		
Versión:	1.0	**Fecha:**	01/09/2016

Revisión y aprobación			
Revisado por:	Responsable de Seguridad		
Aprobado por:	Comité de Seguridad	**Fecha:**	22-03-2017

Lista de distribución	

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio

INDICE

1. OBJETO

El objeto del presente documento es establecer la normativa de uso de los sistemas de información en el Ayuntamiento de Martos (en adelante la Organización), dentro del alcance señalado en el Esquema Nacional de Seguridad.

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

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

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el Usuario final del sistema (informático y papel), debido en gran parte al desconocimiento de la importancia que tiene la seguridad de la información.

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

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

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

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la Organización, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ALCANCE

Esta normativa es de aplicación a todo el ámbito de actuación de la Organización, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la Organización

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, especialmente, el Responsable de Seguridad, los responsables de Sistemas de Información y los propios usuarios,

como actores ambos, en sus respectivas competencias, de la especificación de la normativa de control de acceso, de la implantación técnica de dicha normativa, y del cumplimiento de la misma, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de la Organización.

3. LEGISLACIÓN Y NORMATIVA APLICABLE

Las referencias tenidas en cuenta para la redacción de esta normativa han sido:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Ley 15/1999, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- Documentos y Guías CCN-STIC.

4. ROLES Y RESPONSABILIDADES

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

5. CUERPO DEL DOCUMENTO

5.1. Propiedad y uso de los dispositivos

La Organización facilita a los Usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Propiedad de los recursos. Este equipamiento es propiedad de la Organización y por tanto no está destinado a un uso personal. Como consecuencia de esto, la Organización se reserva el derecho de revisar, sin previo aviso, los equipos y el uso de Internet y el teléfono corporativo que esté haciendo cada Usuario, en caso que existieren indicios de que se está llevando a cabo una utilización indebida. De esta forma el usuario queda informado de que el resultado de los controles efectuados puede ser utilizado para llevar a cabo, en su caso, las actuaciones disciplinarias previstas por la normativa vigente.

Obligaciones de los usuarios. Los Usuarios deben cumplir las siguientes medidas de seguridad para el uso de los ordenadores personales:

Conexión de otros dispositivos	• No está permitido conectar dispositivos que no estén autorizados a la red de la Organización. • Tampoco se pueden conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente.
Ubicación del dispositivo	• No está permitido variar la ubicación física de los dispositivos asignados a una ubicación.
Configuración del dispositivo	• No está permitido alterar la configuración física, configuración de seguridad ni el software de los dispositivos.
Uso de dispositivos y de la red	• Los dispositivos, así como la red de información que la Organización pone a disposición de los usuarios están destinados a permitir el desempeño de las funciones y tareas profesionales que estos tienen encomendadas, estando prohibido el uso para otras finalidades de carácter personal, o bien para la realización de actos desleales o que pudieran ser considerados ilícitos.
Antivirus	• El Usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario deberá notificarlo como una incidencia de seguridad.
Uso de la información	• Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otra distinta del servicio al que está destinada. • El Usuario se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de este Organismo en ordenador propio, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de Seguridad, y se adopten las medidas de seguridad correspondiente. Asimismo, los datos contenidos en este tipo de soportes deben ser suprimidos una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático externo, deberá restringir el acceso y uso de la información que obra en los mismos. • El Usuario deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de la Organización y dispuesto a razón única de las funciones o tareas desempeñadas en la misma. Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el Usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.
Identificación y autenticación	• Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por la Organización son personales e intransferibles,

	siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.
	• Por cuestiones de seguridad no están permitidas prácticas como:
	  ○ Emplear identificadores y contraseñas de otros Usuarios para acceder al sistema y a la red de la Organización.
	  ○ Intentar modificar o acceder al registro de accesos.
	  ○ Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros.

5.2. Uso de la red corporativa

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

Por razones de seguridad, y con el fin de evitar riesgos, los Usuarios deben cumplir las siguientes medidas para el uso de la red corporativa:

Uso de internet	• La utilización de Internet por parte de los Usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de Usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. En este sentido se prohíbe el uso de Internet para fines no relacionados con las funciones encomendadas en cada puesto. • La Organización podrá controlar el uso de acceso a Internet proporcionado. Para ello seguirá un sistema basado en un control de las páginas visitada, lo que podrá suponer el almacenamiento y control de las cookies que se generen. • La normativa completa sobre el uso de Internet puede consultarse en el ANEXO 2 del presente documento.
Uso del correo electrónico	• Se considera el correo electrónico como un instrumento básico de trabajo. • El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones. • Los envíos masivos de información, así como lo correos que se destinen a gran número de usuarios serán solo los estrictamente necesarios que puedan provocar un colapso del sistema de correo.

	• No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. • La Organización se reserva el derecho de que el *Responsable de Seguridad* o el *Responsable del Sistema* pueda revisar y controlar el uso correcto del correo electrónico corporativo. • En caso de ausencia, baja temporal o definitiva, el *Responsable del Departamento* correspondiente podrá consultar su buzón de correo o redireccionar su cuenta con la finalidad de continuar con el normal desarrollo de la actividad de la Organización. • La normativa completa sobre el uso del correo electrónico puede consultarse en el ANEXO 1 del presente documento.
Compartición de contenidos	• Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

5.3. Acceso a aplicaciones y servicios

Tanto el equipamiento informático como todos los recursos facilitados al usuario para la realización de las tareas relacionadas con su puesto de trabajo (tales como teléfonos móviles, aplicaciones, servicios, etc.) son propiedad de la Organización, por lo que deberá hacerse un uso diligente de los mismos. En este sentido se le informa de que podrá revisarse la utilización que cada Usuario esté haciendo de los teléfonos móviles facilitados para el desempeño de su puesto de trabajo. En caso, que existieran indicios acerca del uso indebido de los mismos, podrá realizarse un control de la facturación, así como de los destinatarios de las llamadas realizadas.

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa.

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

Identificación y autenticación	• Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante Usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
Custodia de las contraseñas	• La custodia de la contraseña es responsabilidad del Usuario. Nunca debe utilizarse la cuenta de Usuario asignada a otra persona. • Las contraseñas no deben anotarse, deben recordarse.
Renovación de las contraseñas	• Las contraseñas deben cambiarse periódicamente. Los Usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.

Incidencias con las contraseñas	• Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente.
Bloqueo del puesto de trabajo	• Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas, habilitar el protector de pantalla con bloqueo con contraseña, y apagar los equipos al finalizar la jornada laboral. Excepto en los casos en que el equipo deba permanecer encendido.

5.4. Acceso y tratamiento de datos personales

Regulación. Las anteriores instrucciones serán de aplicación en la observancia del cumplimiento de Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

Concepto. Datos de carácter personal es cualquier información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, relativa a un aspecto/s físico, psíquico, fisiológica, cultural, social o económico de la persona, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Datos de Nivel básico: se aplica a todos los datos de carácter personal y los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando: (i) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. (ii) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad. (iii) Los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Datos de Nivel medio: Datos de solvencia patrimonial o crédito y aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Datos de Nivel alto: Ideología, afiliación sindical, creencias, religión, origen racial, salud, vida sexual, datos derivados de actos de violencia de género.

Obligaciones. Dado que está Ley trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el Usuario, que accede y trata información de carácter personal en el desempeño de las funciones y tareas, deberá atender a las siguientes obligaciones:

Deber de secreto	• Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación que le une con la Organización.
Contraseñas	• Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el Usuario el único responsable de las

	consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. • Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático. • Los usuarios deben utilizar contraseñas seguras. Se entiende que una contraseña es robusta cuando posee, al menos, 8 caracteres (compuestos por letras mayúsculas y minúsculas, dígitos y signos especiales), evitando que la contraseña obtenida sea una palabra de un diccionario, una fecha o, de alguna manera, esté relacionada con el usuario (NIF, nombres propios y apellidos, nombres de mascotas, nombres de ciudades o países, nombres de personajes famosos, deportistas, etc.). Para evitar la problemática derivada de la necesaria memorización de las contraseñas, un mecanismo útil suelen ser los llamados acrósticos, que consisten en seleccionar un carácter de cada palabra de una frase conocida y fácilmente memorizable. Por ejemplo, la frase: “Mi nombre es Napoleón Bonaparte. Tengo 36 años.”, puede generar la siguiente contraseña: MneNB.T36a.
Bloqueo del puesto	• Bloquear la sesión del Usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público o comparta oficina con otros usuarios o no cierre la puerta de su despacho.
Almacenamiento de archivos	• Guardar todos los ficheros de carácter personal empleados por el Usuario, en el espacio de la red informática habilitado por la Organización a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
Manipulación de los archivos	• Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros.
Ficheros temporales	• Ficheros temporales son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. • Los ficheros temporales deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática, o de forma que puedan ser fácilmente localizados.
Correo electrónico	• No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.
Incidencias	• Entre otras acciones, tienen la consideración de incidencia de seguridad las siguientes:

	○ Pérdida de contraseñas de acceso a los Sistemas de Información. ○ Uso indebido de contraseñas. ○ Acceso no autorizado de usuarios a ficheros excediendo sus perfiles. ○ Pérdida de soportes informáticos o documentos en papel con datos de carácter personal. ○ Pérdida de datos por mal uso de las aplicaciones. ○ Ataques a la red. ○ Infección de los sistemas de información por virus u otros elementos dañinos. ○ Fallo o caída de los Sistemas de Información, etc. ○ Documentos que se hallen en papeleras con datos personales. • Se deberán comunicar las incidencias de seguridad de las que tenga conocimiento, que puedan afectar a la seguridad de los datos personales, de acuerdo al procedimiento establecido. Esto resulta también de aplicación a la información en papel.
Soportes informáticos (*pendrives* y discos duros externos USB, CDs, DVDs, disquetes, etc.)	• La salida de soportes que contengan datos de nivel medio o alto fuera de los locales de la Organización debe ser expresamente autorizada. Toda salida de soportes deberá además quedar registrada de acuerdo al procedimiento establecido en la Organización. • La entrada de soportes que contengan datos personales deberá quedar registrada de acuerdo al procedimiento establecido en la Organización. Asimismo, el soporte deberá ser dado de alta en el inventario de soportes de acuerdo al procedimiento establecido en la Organización. • Debe evitarse el uso de unidades de almacenamiento de la información externas para uso privado como por ejemplo disquetes, pendrives, discos duros externos, CD-R, DVD-R, etc. • En caso de necesitar desechar un soporte que contenga datos personales, se destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. Asimismo, el soporte deberá ser dato de baja del correspondiente inventario.

FICHEROS EN PAPEL

En relación con los ficheros en soporte o documento papel, el Usuario deberá observar las siguientes diligencias indicadas anteriormente con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones del Ayuntamiento. Asimismo, con carácter especial y únicamente de aplicación a los ficheros en papel, el Usuario deberá cumplir además con las siguientes diligencias:

Archivadores o dependencias	• Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal. • En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada de trabajo o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
Almacenamiento de documentos	• El archivo de la documentación se realizará siguiendo los criterios establecidos por la Organización, para garantizar su correcta conservación. • Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de cada área de la Organización. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información. • Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos. • No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.
Custodia de documentos	• Cuando los documentos en soporte papel no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso. • Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada de trabajo. • Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes. • Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.
Traslado	• En los procesos de traslado de documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubiera datos de carácter personal. • En caso de cambiar de dependencia, en el proceso de traslado de los documentos en soporte papel, se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal. • Si se envían a terceros ajenos a la Organización datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener

	presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
Destrucción	• No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. • A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio que disponga la Organización.
Registro de accesos	• Se debe mantener un registro de accesos a la documentación con datos de nivel alto (Ej: datos sindicales, salud, etc., siempre y cuando vayan a ser utilizados por varios usuarios.
Incidencias	• Comunicar al Servicio de Sistemas y Comunicaciones las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales. • Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel**,** los sucesos siguientes: ○ Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal. ○ Uso indebido de las llaves de acceso. ○ Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal. ○ Pérdida de soportes o documentos en papel, con datos de carácter personal. ○ Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

5.5. Proceso disciplinario

Se considera un incumplimiento de sus obligaciones por parte del empleado, susceptible de ser sancionado, la inobservancia de las normas y procedimientos contenidos en este documento.

La valoración de las consecuencias del incumplimiento para el infractor, y las medidas a adoptar serán tomadas de conformidad con las normas que regulan la relación laboral entre la empresa y el empleado.

6. ANEXOS/FORMATOS

6.1. Anexo 1. Normas de uso del correo electrónico

6.1.1. Objetivo

El objetivo de la presente Norma es regular el acceso y utilización del correo electrónico (e-mail) por parte de los usuarios de los Sistemas de Información de la Organización, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

6.1.2. Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de la Organización, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de la Organización.

6.1.3. Cuerpo del documento

Concepto. El correo electrónico (e-mail) es un servicio de red para permitir a los usuarios de la Organización enviar y recibir mensajes. Junto con los mensajes también pueden ser enviados ficheros adjuntos.

Caracteres. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

Especificaciones. La Organización, consciente de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes especificaciones:

Responsabilidad	• Los usuarios serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la Organización. • Los usuarios deberán ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por la Organización. • Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la correspondiente autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial. • Los mensajes de correo transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como

	daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.
Uso aceptable	• Como norma general no se utilizará la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades que cada usuario tiene encomendadas en la Organización. • La utilización del correo electrónico por personal externo requiere la previa autorización por escrito de la Dirección. • La forma y contenidos de los correos enviados por el usuario estarán alineados con las normas éticas y de cortesía marcadas por la Organización, y en ningún caso se enviarán correos ofensivos, amenazantes o de mal gusto. • El usuario debe mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados, y todos los archivos adjuntos almacenados en el equipo o unidad de disco habilitada.
Usos no permitidos que implican un riesgo para la seguridad	• La instalación y uso de cualquier otra aplicación de correo electrónico, así como de una versión diferente de la aplicación homologada que no haya sido autorizada e instalada por el personal técnico autorizado. • La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva. • El uso no autorizado de servidores propiedad de la Organización para el envío de correo personal. • El envío masivo de correos publicitarios o de cualquier otro tipo que no guarde relación alguna con las necesidades de negocio de la Organización. Este hecho, además, puede llegar a ser interpretado como “spamming”. • La divulgación, independientemente del formato en que se encuentren, de correos que revelen datos del directorio o de usuarios pertenecientes a la Organización, fuera de los límites laborales establecidos por la misma. • En el caso de se requiera enviar un mensaje de correo electrónico a varios destinatarios, se utilizará preferentemente el campo CCO (copia oculta) para introducir las direcciones de correo de los destinatarios, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación de todos los destinatarios para confirmar que han sido informados.
Diligencia	• Los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos o de dudosa procedencia no serán abiertos, y menos aún los archivos adjuntos que contengan. Su eliminación debe ser inmediata. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.). • No emplear el correo electrónico como medio de comunicación para enviar o recibir información confidencial o que contenga datos de carácter personal de nivel alto (datos de salud, ideología,

	afiliación sindical, religión, creencias, origen racial, vida sexual, violencia de género, fines policiales). Únicamente, y en aquellos casos en los que sea estrictamente necesario, se utilizará este medio, en cuyo caso, se enviará con las medidas de seguridad apropiadas para cada tipo concreto de información mediante la utilización de un software de cifrado, previa autorización expresa del responsable de seguridad. • En la medida de lo posible, desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos. Del mismo modo, limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute. • Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados. • Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada. • Desactivar las características de recordar contraseñas para el navegador. • Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
Incidencias	• Los usuarios deberán comunicar a sus responsables directos sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus.
Monitorización	• La Organización se reserva el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Organización como responsable civil subsidiario.

6.2. Anexo 2. Normas de uso de internet

6.2.1. Objetivo

El objetivo de la presente Norma es regular el uso de internet por parte de los usuarios de los Sistemas de Información de la Organización, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

6.2.2. Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de la Organización, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de la Organización.

6.2.3. Cuerpo del documento

Con carácter general, los usuarios de la Organización disponen de acceso a Internet como herramienta de productividad y conocimiento, así como de mejora de los sistemas de trabajo y búsqueda de información. Esta herramienta es propiedad de la Organización, la cual se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

- Seguridad: debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- Volumen del tráfico externo de datos: garantizando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de la Organización.
- Volumen del tráfico interno de datos: como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- Ética: es ineludible el compromiso que la Organización debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

Responsabilidad	• Internet es un servicio que [nombre de la empresa] pone a disposición de su personal para uso estrictamente profesional. • Los usuarios son los únicos responsables de las sesiones iniciadas en Internet desde sus terminales de trabajo, y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente Normativa. • El acceso a Internet por personal externo requiere la previa autorización por escrito de la Dirección.

Monitorización	• La Organización se reserva el derecho a filtrar el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios propiedad de la Organización, así como a monitorizar y registrar los accesos realizados desde los mismos. En caso de que un usuario considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable directo para que éste gestione el acceso correspondiente.
Usos no permitidos que implican un riesgo para la seguridad	• En ningún caso se modificarán las configuraciones de los navegadores (opciones de Internet) de los equipos ni la activación de servidores o puertos sin la autorización expresa. Todos los equipos que así lo estima la empresa, ya están configurados para su acceso a Internet. • Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Organización. • No se permite el almacenamiento en los equipos de archivos y contenidos personales descargados vía Internet, especialmente aquellos que violen la legislación vigente relativa a Propiedad Intelectual. Los usuarios deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos o de red de la Organización. • Se prohíbe el uso de Internet mediante los recursos informáticos o de red de la empresa con fines recreativos, así como para obtener o distribuir material violento o pornográfico, o para obtener o distribuir material incompatible con los valores de la Organización. • El uso de chats o programas de conversación en tiempo real no está permitido. • La descarga de software ejecutable desde internet.
Incidencias	• Cualquier incidente de seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al responsable directo oportuno

7. REFERENCIAS