

Sexto: Notifíquese en legal forma al Interesado, al Instructor y a la Secretaria del expediente.

La Concejala-Delegada de Presidencia, Relaciones Institucionales y Modernización de la Administración. M.^a Victoria Cañal Hernández-Díaz. Ante mí, El Secretario General.

Lo que traslado para su conocimiento. Mairena del Aljarafe a 7 de febrero de 2014. El Secretario General. Recibí el Duplicado.

Lo que se hace público para general conocimiento.

En Mairena del Aljarafe a 3 de marzo de 2014.—El Concejala-Delegada de Presidencia, Relaciones Institucionales y Modernización de la Administración, Victoria Cañal Hernández-Díaz.

253W-3001

UTRERA

Don Juan Borrego López, Secretario General del Excmo. Ayuntamiento de esta ciudad.

Hace saber que: Por el Pleno de la Corporación, en sesión ordinaria celebrada el día 11 de julio de 2013, se adoptó el acuerdo de aprobar «Documento de Seguridad de la Información Corporativa del Excmo. Ayuntamiento de Utrera.», con el siguiente tenor literal:

«Visto acuerdo del Excmo. Ayuntamiento Pleno en sesión ordinaria celebrada el día catorce de noviembre de dos mil trece por el que se aprobó inicialmente el Documento de Seguridad de la Información Corporativa del Excmo. Ayuntamiento de Utrera.

Visto que dicho acuerdo se publicó en el «Boletín Oficial» de la provincia de Sevilla número 6, de 9 de enero de 2014 a los efectos de que pudieran formularse cuantas alegaciones se estimasen convenientes durante el plazo de treinta días a partir del día siguiente al de la publicación en el citado boletín.

Visto Certificado del Secretario General de fecha catorce de febrero de dos mil catorce en el que consta que durante la exposición al público no se ha producido reclamación/alegación alguna contra el mismo.

Visto que la Ley 7/85, de 2 de abril, Reguladora de las Bases de Régimen Local, en su artículo 49 recoge que en el caso de que no se hubiera presentado ninguna reclamación o sugerencia a la aprobación inicial, se entenderá definitivamente adoptado el acuerdo hasta entonces provisional.

Por el presente, resuelvo:

Primero.—Aprobar definitivamente el Documento de Seguridad de la Información Corporativa del Excmo. Ayuntamiento de Utrera, atendiendo a lo dispuesto en el artículo 49 de la Ley 7/85, de 2 de abril, Reguladora de las Bases de Régimen Local.

Segundo.—Publíquese el acuerdo y texto íntegro de la Ordenanza en el «Boletín Oficial» de la provincia de Sevilla, en cumplimiento de lo dispuesto por el artículo 70.2 del mismo cuerpo legal.

Lo decreta y firma el Sr. Alcalde-Presidente, ante mí el Secretario General, que doy fé.

En Utrera a 20 de febrero de 2014.»

Lo que se hace público, significándole que contra las disposiciones administrativas de carácter general no cabrá recurso en vía administrativa (Art. 107.3, de la Ley 30/92, de 26 de noviembre sobre el Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común). Por lo que sólo podrá interponer recurso Contencioso-Administrativo ante la Sala del Tribunal Contencioso-Administrativo en el plazo de 2 meses (Art. 46.1 Ley 29/1998 Reguladora de la Jurisdicción Contenciosa-Administrativa), a contar así mismo de la fecha de su publicación en el «Boletín Oficial» de la provincia.

*Documento de seguridad de la información corporativa del Excmo. Ayuntamiento de Utrera.
7 de noviembre de 2013.—V.1*

1) Introducción

El presente documento desarrolla el Documento de Seguridad de la Información (en adelante Documento) definido por el Ayuntamiento de Utrera en materia de Sistemas de Información (en adelante SSII), entendiéndose éstos como el conjunto de ficheros automatizados y no automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos, así como todas aquellas personas que tienen acceso a la información y a los sistemas.

Así mismo, responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007 de 21 de Diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal, así como lo dispuesto en la propia Ley Orgánica 15/1999 de 13 de Diciembre y a lo dispuesto en la Ordenanza Reguladora de la Seguridad de la Información, Creación, Modificación y Supresión de los ficheros de carácter personal del Excmo. Ayuntamiento de Utrera.

Y establece los métodos y procedimientos a seguir por parte del personal del Ayuntamiento tendentes a conseguir una adecuada protección de los Activos de Información (entre ellos los datos personales), así como su obtención, tratamiento, transmisión, etc.

La Seguridad de la Información consiste en un conjunto de medidas, controles, procedimientos y acciones destinados a cumplir con los aspectos básicos esenciales para el buen servicio al ciudadano, el cumplimiento de la legalidad vigente y la imagen de la propia entidad:

- Confidencialidad: la información debe ser conocida exclusivamente por las personas autorizadas, en el momento y forma prevista.
- Integridad: la información tiene que ser completa, exacta y válida, siendo su contenido el previsto de acuerdo con unos procesos predeterminados, autorizados y controlados.
- Disponibilidad: la información debe estar accesible y ser utilizable por los usuarios autorizados en todo momento, debiendo estar garantizada su propia persistencia ante cualquier eventualidad.
- Eficiencia y eficacia administrativa por cuanto los recursos deben ser bien administrados.

La definición, desarrollo e implantación de los aspectos contenidos en este Documento da cobertura a todos los requerimientos establecidos en Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), así como los exigidos en el Reglamento de desarrollo de la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal.

Los acrónimos utilizados en este documento son los siguientes:

DCPs: Datos de Carácter Personal.

APD: Agencia de Protección de Datos.

CPD: Centro de Proceso de Datos.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal.

Reglamento: Reglamento de desarrollo de la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal (aprobado en el RD 1720/2007).

R.G.P.D.: Registro General de Protección de Datos.

ENS: Esquema Nacional de Interoperabilidad.

CCN: Centro Criptológico Nacional.

2) *Ámbito de aplicación*

2.1) *Ámbito funcional*

Este documento se aplicará en el Ayuntamiento de Utrera respecto a sus recursos de información y conocimiento, en la extensión y detalle que se describen en el mismo.

En este documento destaca la política de seguridad y las directrices generales de seguridad definidas por la organización para los ficheros que contienen datos de carácter personal e información corporativa. Estas políticas, normas y procedimientos se aplican a todos aquellos ficheros y recursos, protegidos o no, que contengan o traten datos automatizados y no automatizados.

Asimismo, el documento recoge las medidas técnicas que garantizan la seguridad física de los lugares, instalaciones, muebles, etc. donde se almacena información sensible del Ayuntamiento.

2.2) *Ámbito personal*

La Política de Seguridad y las Directrices Generales de Seguridad contenidas en el presente documento son de obligado cumplimiento para todo el personal, comprendiendo éste a los siguientes:

- Funcionario público: Todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas.
- Empleado público: quienes desempeñan funciones retribuidas en el Ayuntamiento de Utrera al servicio de los intereses generales: funcionarios de carrera, funcionarios interinos, personal laboral, ya sea fijo, por tiempo indefinido o temporal y personal eventual.
- Personal de proveedores de servicio externos, cuando sean usuarios de los Sistemas de Información del Ayuntamiento.
- Personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el Ayuntamiento de Utrera y que utilice o posea acceso a los Sistemas de Información del Ayuntamiento.

2.3) *Ámbito material*

La Política de Seguridad y las Directrices Generales de Seguridad contenidas en el presente documento son de obligatoria aplicación a los sistemas y soportes que contienen información personal en el Ayuntamiento de Utrera, comprendiendo éstos los siguientes:

1. Sistemas de información para el tratamiento automatizado de los datos.
2. Soportes físicos con capacidad para el almacenamiento de datos.
3. Servicios prestados por el Ayuntamiento de Utrera.

3) *Política de Seguridad*

Alcaldía Presidencia

Asunto: Política de Seguridad de la Información

La preservación de todo lo relacionado con la información que genera el conjunto de documentos, materiales y equipos, instalaciones, personas, sistemas informáticos, etc. y cuyo conocimiento por terceros no es deseado, se denomina Seguridad de la Información, información que es necesaria preservar para el óptimo servicio al ciudadano, además de que su quebranto pueda tener graves repercusiones legales, iría contra la buena imagen, la seguridad y el adecuado funcionamiento del Ayuntamiento de Utrera.

En el documento de Directrices Generales de Seguridad, que es parte del Documento de Seguridad, están definidas las normas de actuación y gestión adecuada para el cumplimiento de las mismas en el Ayuntamiento, que aseguran un adecuado equilibrio entre las necesidades para el desempeño de la función pública por parte de los empleados públicos municipales, las exigencias de seguridad y el respeto a las leyes vigentes.

La aplicación de estas directrices permitirá garantizar la protección de la información y forman parte del conjunto de medidas, controles y procedimientos destinados a cumplir con los aspectos básicos que son esenciales para el funcionamiento de la entidad, el cumplimiento de la legalidad vigente y la propia imagen: confidencialidad, integridad, disponibilidad, disponibilidad y autenticidad.

Todo el personal del Ayuntamiento deberá cumplir las directrices, normas y procedimientos que se regulan en el Documento de Seguridad, y como consecuencia de ello asumirá el deber de colaboración con el Ayuntamiento en el interés de que no se produzcan alteraciones o violaciones de estas reglas, así como cumplir las órdenes y resoluciones emanadas por la organización de la Seguridad de la Información.

Todas las personas que prestan sus servicios en el Ayuntamiento deben conocer y asumir las obligaciones respecto del uso correcto de los recursos informáticos recogidas en las Directrices Generales de Seguridad. El incumplimiento de estas obligaciones por parte del personal podrá dar lugar a responsabilidad disciplinaria, y al ejercicio de los procedimientos legales por el Ayuntamiento para su exigencia. Francisco Jiménez Morales.—Alcalde – Presidente del Excmo. Ayuntamiento de Utrera.-

4) *Normas Generales de Seguridad.*

4.1) *Cumplimiento de las obligaciones.*

Con objeto de dar debido cumplimiento a lo establecido en la legislación vigente, el Ayuntamiento de Utrera impone a su personal el cumplimiento de las normas que se exponen a continuación.

Una vez recibido el presente documento todos los funcionarios y empleados públicos (usuarios) procederán a su lectura, y en el caso de dudas sobre su contenido, se pondrán en contacto con el Responsable de Seguridad para su aclaración.

Comprendidas las normas y aclaradas las dudas que puedan surgir, todos los funcionarios y empleados municipales aceptarán su contenido, asumiendo las obligaciones que en ellas se contienen.

Su incumplimiento podrá suponer la adopción de las medidas disciplinarias que, en su caso, correspondan.

4.2) *Normas sobre ficheros que contienen datos de carácter personal.*

1) Todos los/as empleados/as están obligados a facilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición conforme al Título III del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2) Queda prohibido sin el previo consentimiento del Responsable de los Ficheros:

- * La creación de ficheros que contengan datos de carácter personal.
- * Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias.
- * Utilizar ficheros con datos personales que el Ayuntamiento no haya comunicado y registrado ante la Agencia Española de Protección de Datos.

3) Transmitir, alojar o recepcionar información que contenga datos de carácter personal, confidencial o protegida propia del Ayuntamiento de Utrera en servidores externos o internos al Ayuntamiento. Para llevar a cabo alguna de estas operaciones se requerirá la previa tramitación del expediente administrativo correspondiente.

Gestión de ficheros que contienen datos de carácter personal.

La gestión de los ficheros que contienen datos de carácter personal en el Excmo. Ayuntamiento de Utrera será realizada por medio de los siguientes procedimientos:

1) *Procedimiento de creación, modificación de ficheros de carácter personal.*

Será utilizado para la creación y modificación de ficheros municipales que contengan datos de carácter personal. La LOPD obliga a las AAPP a declarar los ficheros que usan para la gestión de los distintos expedientes administrativos y que contienen datos de carácter personal. Para dicha circunstancia el Ayuntamiento pone a disposición de las distintas delegaciones municipales el uso del procedimiento citado para la creación y modificación de ficheros que en todo caso deberá estar conforme al Título V del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2) *Procedimiento de acceso, modificación, cancelación de datos de carácter personal.*

Conforme a lo dispuesto en la LOPD, el RLPD, las personas pueden ejercer los derechos de acceso, rectificación, cancelación y oposición respecto de los datos que obren en poder de las Administraciones públicas. Dichos derechos deberán poderse ejercer mediante el procedimiento de referencia indicado en el artículo 25 del Título III del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3) *Procedimiento para tratamiento de datos por cuenta de terceros.*

Conforme a la LOPD y el RLPD y el Esquema Nacional de Seguridad, el Ayuntamiento debe respetar los derechos de las personas, la disponibilidad, autenticidad, confidencialidad, integridad y trazabilidad de la información y los servicios. Para lo cual, y conforme a la LOPD, al articulado que desarrolla las relaciones con el encargado del tratamiento, las normas técnicas de desarrollo del ENS y las recomendaciones del Centro Criptológico Nacional, el Ayuntamiento de Utrera habilita este procedimiento al objeto de cumplir sus deberes.

En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero, así como informe del Responsable de Seguridad que previo análisis de los riesgos comprobará:

- i) La inexistencia de trabas legales para ello.
- ii) Verificará la suscripción de contrato o convenio expreso entre el Ayuntamiento de Utrera y la empresa responsable de la prestación del servicio.
- iii) El cumplimiento por parte de la empresa responsable de lo previsto en el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.
- iv) El cumplimiento de lo previsto en la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.
- v) El acuerdo de confidencialidad y de nivel de servicio que procedan.
- vi) El seguimiento de la Guía CCN-STIC-823 del Centro Criptológico Nacional

A la vista de los documentos obrantes en el expediente, el Responsable del Fichero quién decidirá sobre la procedencia o no de acceder a lo solicitado.

4) *Procedimiento para transmitir, alojar o recepcionar información hacia o desde servidores externos al Ayuntamiento.*

En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero, así como informe del Responsable de Seguridad que previo análisis de los riesgos comprobará:

- i) La inexistencia de trabas legales para ello.
- ii) Verificará la suscripción de contrato o convenio expreso entre el Ayuntamiento de Utrera y la empresa responsable de la prestación del servicio.
- iii) El cumplimiento por parte de la empresa responsable de lo previsto en el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.
- iv) El cumplimiento de lo previsto en la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.
- v) El acuerdo de confidencialidad y de nivel de servicio que procedan.
- vi) El seguimiento de la Guía CCN-STIC-823 del Centro Criptológico Nacional

El informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de la solicitud.

4.3) *Control de actuaciones sobre las bases de datos del Ayuntamiento de Utrera*

- 1) El Ayuntamiento de Utrera habilitará Sistemas de Información cuyo acceso y/o modificación de la información contenida en los mismos quedará registrada en una Base de Datos, lo que permitirá su ulterior auditoría.
- 2) Las modificaciones de los datos deben realizarse sólo por parte de los usuarios autorizados y deberán estar siempre respaldadas por un expediente administrativo que justifique los cambios.
- 3) La carga de ficheros de información deben ser debidamente registrados en los registros de entrada/salida, de acuerdo con los procedimientos establecidos.
- 4) Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, desde fuera de las aplicaciones del Ayuntamiento de Utrera sin la autorización previa del Responsable de los Ficheros.

Gestión de las actuaciones sobre las bases de datos del Ayuntamiento de Utrera.

La gestión de las actuaciones sobre las bases de datos del Excmo. Ayuntamiento de Utrera que requiera autorización previa, será realizada por medio del siguiente procedimiento:

1) Procedimiento para la autorización de la actualización de la información contenida en las bases de datos municipales desde fuera de las aplicaciones internas del Ayuntamiento de Utrera.

2) Procedimiento para la recuperación de datos, ficheros y servicios de las copias de seguridad.

En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero. El Responsable de Seguridad dejará constancia de la recuperación en el registro correspondiente.

4.4) *Normas sobre el uso adecuado de los bienes del Ayuntamiento.*

- 1) El sistema informático, la red corporativa, las máquinas, los terminales, los datos y el software utilizados por cada usuario son propiedad del Ayuntamiento de Utrera y están disponibles exclusivamente para cumplir las obligaciones, fines, planes y objetivos de la Organización y el propósito para el que fueron diseñados e instalados.
- 2) El Ayuntamiento de Utrera facilitará 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 el Ayuntamiento pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.
- 3) Los usuarios tienen acceso autorizado únicamente a aquellos datos y recursos que precisan para el desarrollo de sus funciones.
- 4) Los bienes municipales podrán ser inspeccionados en cualquier momento por el Responsable de Seguridad y el personal a sus órdenes. De la inspección podrá derivarse, en su caso, el correspondiente expediente disciplinario en el que quedará salvaguardado el derecho al honor, la intimidad personal de los empleados municipales y el pleno ejercicio de sus derechos.
- 5) El usuario tendrá la obligación de utilizar los programas antivirus corporativos y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- 6) Usos específicamente prohibidos.
 - a) Usar los bienes del Ayuntamiento para usos distintos del desempeño del puesto de trabajo.
 - b) Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.)
 - c) Utilización de cualquier tipo de software dañino.
 - d) Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
 - e) Requiere autorización la conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por el Ayuntamiento de Utrera.
 - f) Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por la Delegación de Nuevas Tecnologías.
 - g) Requiere autorización expresa, la utilización de dispositivos USB, teléfonos móviles u otros elementos, con capacidad para Internet.
 - h) Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.
 - i) Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
 - j) Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
 - k) Destruir, alterar, inutilizar o dañar los datos, programas o documentos del Ayuntamiento o de terceros.
 - l) Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos del Ayuntamiento o de terceros.
 - m) Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros.
 - n) Borrar cualquiera de los programas instalados legalmente en la red.
 - ñ) Introducir en la red corporativa contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos del Ayuntamiento.
 - o) Modificar la configuración de las máquinas puestas a disposición del funcionario o empleado público.
 - p) Abrir los equipos o máquinas (hardware) para realizar cualquier tarea sobre ellos.
 - q) Agregar o retirar partes o componentes de los mismos.

Gestión para la utilización adecuada de los recursos.

- 1) Los equipos informáticos serán asignados y gestionados por la Delegación de Nuevas Tecnologías.
- 2) Únicamente el personal autorizado por la Delegación de Nuevas Tecnologías podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información del Ayuntamiento de Utrera. Cuando se precise instalar dispositivos no provistos por el Ayuntamiento de Utrera deberá solicitarse autorización previa a la Delegación de Nuevas Tecnologías.
- 3) Cada nuevo usuario que se incorpore a la organización y así lo precise, la Delegación de Nuevas Tecnologías le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales. Para el alta de nuevos usuarios, se requerirá: Nombre, apellidos y NIF, Ubicación, teléfono y dirección de correo electrónico, Área a la que se incorpora, Servicios a los que requiere acceso, aplicaciones y perfiles.
- 4) El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata a la Delegación de Nuevas Tecnologías, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados y los permisos de acceso que hasta ese momento tuviere. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por el Ayuntamiento de Utrera 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.

La gestión de la utilización adecuada de los recursos y la incorporación de nuevos usuarios y la baja de los existentes se realizará por medio de los siguientes procedimientos:

- 1) Procedimiento de autorización de acceso, modificación, cancelación a recursos.
- 2) Procedimiento de control de acceso a aplicaciones y sistemas.
- 3) Identificación y autenticación de usuarios.
- 4) Asignación, distribución y almacenamiento de contraseñas.

Todos los procedimientos anteriores deberán contener en su expediente solicitud formulada por el interesado con el visto bueno del Responsable Interno del Fichero, recurso y/o aplicación.

Sólo requerirá informe del Responsable de Seguridad en el caso de los procedimientos de autorización de acceso, modificación, cancelación a recursos y control de acceso a aplicaciones y sistemas.

Del informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de acceder a lo solicitado.

4.5) Normas específicas para equipos portátiles y móviles.

- 1) Los equipos portátiles y móviles (ordenadores, teléfonos, tabletas, ...) serán asignados por la Delegación de Nuevas Tecnologías.
- 2) Este tipo de dispositivos estará bajo la custodia del usuario o tenga autorización para su uso quién deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- 3) La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la Delegación de Nuevas Tecnologías para la adopción de las medidas de seguridad que correspondan.
- 4) Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales.
- 5) Los usuarios de estos equipos se responsabilizarán de que no sean usados por terceras personas ajenas al Ayuntamiento de Utrera o no autorizadas para ello.
- 6) Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).
- 7) Como norma general, los equipos portátiles se configurarán por defecto con todos los canales, puertos y sistemas de comunicaciones de salida de información bloqueados (WiFi, Bluetooth, USB's, CD, DVD, tarjetas de red, etc...). Por petición justificada dirigida a la Delegación de Nuevas Tecnologías, se podrán habilitar algunas o todas las funciones de salida de información.
- 8) Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá a la Delegación de Nuevas Tecnologías llevar a cabo estas modificaciones.
- 9) Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá a la Delegación de Nuevas Tecnologías, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

Gestión de la cesión temporal de equipos portátiles y móviles.

La gestión de la cesión temporal de los equipos portátiles y móviles, se realizará por medio de los siguientes procedimientos:

- 1) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

La sustitución de recursos autorizados previamente deberán ser comunicados al órgano resolutorio del procedimiento de autorización.

4.6) Normas de uso de memorias portátiles, discos, lápices USB, CDROM Y DVD.

- 1) Con carácter general, el uso de memorias USB en el Ayuntamiento de Utrera no está autorizado. En su caso, la autorización deberá solicitarse siguiendo el procedimiento habilitado al efecto. Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. 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 el Ayuntamiento de Utrera, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario del Ayuntamiento de Utrera, no debiendo ser usados fuera de éstos.
- 2) Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. La Delegación de Nuevas Tecnologías podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas del Ayuntamiento de Utrera unidades de almacenamiento en red, que podrán usarse para tal propósito. La pérdida o sustracción de una memoria USB, deberá ponerse en conocimiento de la Delegación de Nuevas Tecnologías, de forma inmediata.

3) Con carácter general, el uso de equipos grabadores de CDs y DVDs en el Ayuntamiento de Utrera no está autorizado. Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo estarán deshabilitados. En su caso, la autorización deberá proporcionarse siguiendo el procedimiento habilitado al efecto.

Gestión de la autorización para el uso de memorias portátiles, discos, lápices USB, ETC.

La gestión de la autorización para el uso de memorias portátiles, discos, lápices usb, CDROM y DVD o cualquier dispositivo con capacidad para el almacenamiento de datos se realizará por medio de los siguientes procedimientos:

1) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

4.7) *Normas de uso adecuado del correo electrónico.*

1) Todos los usuarios contarán para el desempeño de su actividad profesional, de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.

2) Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por el Ayuntamiento de Utrera.

3) Los buzones de correo se deben configurar con un tamaño para almacenamiento limitado (200MB). El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos.

4) Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas, deberá cumplir los requisitos establecidos en el Documento de Seguridad y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

5) La dirección de correo que asigna el Ayuntamiento tiene como propósito su utilización profesional, quedando prohibida su utilización personal.

6) Es responsabilidad de cada usuario seguir las directrices establecidas respecto al correo electrónico.

7) Cualquier correo de procedencia dudosa o desconocida podrá y deberá ser suprimido.

8) Cada usuario deberá realizar borrados periódicos a fin de no saturar el servicio de correo.

9) Usos específicamente prohibidos:

a) Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.

b) Enviar o reenviar mensajes en cadena o de tipo piramidal.

c) Enviar mensajes de correo electrónico de forma masiva excepto en aquellos casos cuya finalidad sea realmente de interés general.

d) Enviar mensajes con fines comerciales o publicitarios, y en general, que pudieran saturar el sistema de correo.

e) Revelar a terceros el contenido de cualquier dato reservado o confidencial propiedad del Ayuntamiento de Utrera o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

f) Utilizar para propósitos que puedan influir negativamente en la imagen del Ayuntamiento de Utrera, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

g) El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, etc... que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

h) Utilizar el correo electrónico para fines distintos a los derivados de las actividades profesionales del usuario.

Gestión de las normas del correo electrónico.

La gestión de las incidencias sobre el correo electrónico será a través del procedimiento:

1) Procedimiento de gestión de incidencias

Para la creación de una cuenta de correo personal se hará a través de:

2) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

4.8) *Normas de uso adecuado de Internet.*

1) El usuario está obligado a utilizar la red corporativa y la Intranet del Ayuntamiento y sus datos sin incurrir en actividades que puedan considerarse ilícitas o ilegales, que infrinjan los derechos de la entidad o de terceros, o que puedan atentar contra la moral o las adecuadas normas de uso de las redes telemáticas.

2) El uso del sistema informático del Ayuntamiento para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de éste, y, en concreto, a los cometidos del puesto de trabajo.

3) Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en el Documento de Seguridad y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

4) El Ayuntamiento de Utrera se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa. De la inspección podrá derivarse, en su caso, el correspondiente expediente disciplinario en el quedará salvaguardado el derecho al honor, la intimidad personal de los empleados municipales y el pleno ejercicio de sus derechos.

5) El acceso a redes públicas de telecomunicaciones se restringirá a los cometidos del puesto de trabajo. En este sentido el Ayuntamiento de Utrera aprobará las puertos, categorías, catálogo de ficheros, protocolos, y tecnologías generales de acceso a las redes públicas de comunicaciones. Dichas categorías se adaptarán a las necesidades del Ayuntamiento de Utrera atendiendo a los criterios recomendados por el RD 3/2010 de 8 de Enero, por el que se aprobó el Esquema Nacional de Seguridad (ENS).

6) Usar Internet para fines profesionales. Internet es una herramienta más de las utilizadas por los usuarios del Ayuntamiento de Utrera. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales, con las excepciones o precisiones que se señalen.

7) Está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno del Ayuntamiento de Utrera, sus recursos, estructura, etc.

8) Observar las restricciones legales que sean de aplicación. Antes de utilizar una información obtenida de Internet, los usuarios deberán comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.

9) Realizar descargas sólo si se tiene autorización. En este caso, se limitará su descarga y reproducción al ámbito estrictamente profesional.

10) No descargar código o programas no confiables. Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Tales actividades serán acometidas, de manera exclusiva, por la Delegación de Nuevas Tecnologías.

11) Asegurar la autenticidad de la página visitada. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser.

12) Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad. Comprobar la seguridad de la conexión. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado.

13) Cerrar las sesiones al terminar la conexión. Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información, ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otros usuarios tengan acceso a las cuentas de los usuarios que no hubieren cerrado correctamente las sesiones. La mayoría de los sitios web disponen de una opción de «desconexión», «logout» o similar que conviene utilizar.

Gestión adecuada de Internet.

La gestión de la autorización para la gestión adecuada de internet se realizará por medio del siguiente procedimiento:

1) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

Para problemas relacionados con el acceso, uso de aplicaciones a través de navegadores web se deberá hacer a través de.

2) Gestión de incidencias.

4.9) *Normas sobre propiedad intelectual e industrial.*

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como introducir, descargar de Internet, usar, reproducir, ceder, transformar o comunicar públicamente cualquier otro tipo de obra o invención protegida por la propiedad intelectual o industrial sin la debida autorización.

4.10) *Normas sobre la propiedad de la información.*

1) Toda la información albergada en la red corporativa del Ayuntamiento, en todas sus dependencias, en formato electrónico o papel es propiedad del Ayuntamiento.

2) Cualquier persona al finalizar su relación profesional, funcional o electiva con el Ayuntamiento de Utrera deberá mantener estricta reserva y no divulgará, utilizará ni publicará, a través de cualquier medio de comunicación, ni directamente ni a través de terceras personas, información recibida en virtud del desempeño de su relación profesional, ya sea referida al propio Ayuntamiento, otros organismos, ciudadanos o personal relacionado con éste, salvo que tal divulgación, utilización o publicación le sea requerida expresamente por escrito por el Ayuntamiento debido a motivos de trabajo.

3) El usuario será responsable con 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 de información sensible, confidencial o protegida.

Gestión de la información propiedad del Ayuntamiento.

1) Procedimiento de remisión de información propiedad del Ayuntamiento.

Se deberá usar el procedimiento para transmitir, alojar o recepcionar información hacia o desde servidores externos al Ayuntamiento, para tener autorizado por norma general de la remisión de una tipología concreta de información.

Una vez autorizada que la información referida se puede remitir habitualmente a otras administraciones, personas físicas o jurídicas para cumplir alguno de los fines del Ayuntamiento y sus contratos deberá quedar materializada en el Registro de Salida del Ayuntamiento de Utrera previa autorización del Responsable Interno del Fichero.

4.11) *Normas sobre la identificación y autenticación de usuarios.*

1) Todo el personal deberá acceder a los recursos y sistemas de información mediante los mecanismos que el Ayuntamiento de Utrera pone a su disposición:

a) Un identificador y una contraseña de acceso.

b) Certificado digital.

2) La contraseña de acceso debe ser secreta. Cada usuario es responsable de la utilización que se realice con su identificador y contraseña. Este identificador deberá ser único y personal.

3) Queda prohibido comunicar, compartir o facilitar con otra persona el identificador de usuario y la contraseña proporcionados por el Ayuntamiento, incluido tanto el personal del departamento o servicio como personas ajenas a éste.

4) Los usuarios no deben mantener por escrito su identificador y/o contraseña a la vista o al alcance de terceros.

5) Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del Servicio de Informática, con el fin de que le asigne una nueva clave de forma inmediata.

6) En casos excepcionales en los que sea necesario continuar con las funciones que realiza una persona ausente (debido a una baja, vacaciones, viaje o ausencia temporal no prevista), se podrá solicitar al Servicio de Informática, por escrito, el acceso a los datos a los que está autorizada la persona ausente.

Procedimientos de identificación y autenticación de usuarios.

La identificación y autenticación de usuarios se realizará por medio del siguiente procedimiento:

- 1) Procedimiento de gestión de usuarios; altas, modificaciones y bajas.
- 2) Procedimiento de acceso excepcional a los datos autorizados para otro empleado/a municipal.
- 4.12) *Normas para preservar la autenticidad, integridad, y confidencialidad de los datos.*

1) Para preservar la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos sustentados por aplicaciones corporativas, todos los cambios funcionales, de versión, inclusión de nuevas funcionalidades deberán ser debidamente autorizados.

2) Para preservar la integridad de los datos, el usuario se compromete a no introducir software no autorizado ni programas que contengan virus, caballos de Troya o bombas lógicas o cualquier elemento que ponga en peligro la seguridad.

3) Los usuarios deben utilizar únicamente las versiones de software proporcionadas por el Ayuntamiento y seguir sus normas de utilización.

4) En el caso de entrar en conocimiento de información que no sea de libre difusión, en cualquier tipo de soporte, deberá entenderse que dicho conocimiento es estrictamente temporal mientras dure la función encomendada, con la obligación de secreto o reserva indefinidas y sin que ello le confiera derecho alguno de posesión, titularidad o copia del mismo. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieren originado su uso.

5) 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.

6) 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.

7) Los soportes de información que vayan a ser reutilizados o causen baja deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación. Estos soportes deberán entregarse a la Delegación de Nuevas Tecnologías.

8) 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.

9) Queda expresamente prohibido:

- a) Efectuar la instalación en los Sistemas de Información de software no autorizado descargado de Internet. El Departamento de Informática es el único autorizado a descargar programas de Internet, vídeos, fotos o cualquier material, siempre que se justifique su utilidad para el desempeño de sus funciones y una vez comprobada la seguridad de los archivos.
- b) Instalar software en la red o en el PC sin autorización previa y escrita.
- c) Inhabilitar los mecanismos de control de su PC.
- d) Retirar software de la oficina sin autorización escrita.
- e) Modificar la configuración de sus equipos sin previa autorización escrita. Las modificaciones de la configuración, especialmente en lo referente a los recursos compartidos pueden ocasionar problemas de seguridad.
- f) Mantener el registro del software instalado con fecha de instalación y actualización.
- g) Formatear los equipos.
- h) Como medida de protección de la información propia, confiada o tratada por el Ayuntamiento de Utrera, está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada.
- i) 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 el Ayuntamiento de Utrera (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.
- j) El uso de medios particulares para el acceso a redes de telecomunicaciones en el desempeño del puesto de trabajo en la dependencias municipales.

Procedimientos para preservar la autenticidad, integridad y confidencialidad de los datos.

Para modificar, o añadir funcionalidades de aplicaciones hay que estar a los dispuesto en:

- 1) Procedimiento de gestión de cambios de aplicaciones.

En todo caso deberá constar en el expediente solicitud del interesado con el visto bueno del Responsable Interno del Fichero seguido del informe correspondiente del Responsable de Seguridad e informe del técnico que corresponda en el que debe constar:

* La aplicación del Título IV del Reglamento Regulator de la Administración Electrónica del Ayuntamiento de Utrera a los cambios/mejoras funcionales solicitados.

* La aplicación de la normativa vigente en materia de Administración Electrónica y su normativa de desarrollo.

- 2) Procedimiento de gestión de la configuración.

4.13) Normas de uso adecuado de los equipos e instalación de software.

1) Los usuarios sólo deben utilizar en su actividad laboral y para el desempeño del puesto de trabajo el hardware y los equipos propiedad del Ayuntamiento.

2) Únicamente el personal de soporte técnico autorizado por la Delegación de Nuevas Tecnologías podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

3) Excepción a esta norma serán aquellas herramientas de uso común incluidas en el Catálogo de Aplicaciones Autorizadas del Ayuntamiento de Utrera, descargables desde los servidores internos del Ayuntamiento de Utrera.

4) Todo usuario podrá solicitar la inclusión de una aplicación en dicho Catálogo de Aplicaciones Autorizadas para su estudio por parte de la Delegación de Nuevas Tecnologías. 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.

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

6) En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por la Delegación de Nuevas Tecnologías, especialmente aquellas relacionadas con la seguridad.

7) Está prohibido:

- a) Abrir los equipos o máquinas (hardware) para realizar cualquier tarea sobre ellos.
- b) Agregar o retirar partes o componentes de los mismos.
- c) Retirar los equipos de las instalaciones del Ayuntamiento sin previa autorización escrita.

Procesos para gestionar los equipos e instalación de software.

Para problemas relacionados con el uso de equipos y aplicaciones se deberá hacer a través de:

- 1) Gestión de incidencias.
- 2) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

4.14) *Normas de uso de impresoras, fotocopiadoras, faxes y escáneres.*

1) 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 el Ayuntamiento de Utrera.

2) 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. Nunca podrá olvidarse de 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. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de la Delegación de Nuevas Tecnologías.

3) 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.

4) Dependiendo de la tipología de la información hallada, podrá abrirse el correspondiente incidente de seguridad.

5) 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. Nunca podrá olvidarse de 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. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de la Delegación de Nuevas Tecnologías.

Procedimientos para la gestión impresoras, fotocopiadoras, faxes y escáneres.

Para problemas relacionados con el uso de impresoras, fotocopiadoras, faxes y escáneres se deberá hacer a través de:

1) Gestión de incidencias.

4.15) *Devolución de documentos, ficheros y materiales.*

1) Cualquier tipo de información (incluidas sus copias) o material de cualquier naturaleza (ordenador, impresora, portátiles, teléfono, etc.) a los que haya tenido acceso la persona durante la vigencia de su relación profesional, funcional o electiva con el Ayuntamiento, será propiedad exclusiva del Excmo. Ayuntamiento de Utrera.

2) Todo lo anterior será entregado al Responsable de Seguridad de forma inmediata a la finalización de la relación.

Procedimiento de devolución de documentos, ficheros y recursos.

Para la gestión de la devolución de documentos, ficheros y materiales se deberá hacer a través de:

1) Procedimiento de autorización de acceso, modificación y cancelación a recursos.

4.16) *Normas sobre la gestión de incidencias.*

1) Es obligación de todo el personal notificar cualquier incidencia, presunción o sospecha de incidencia que se produzca en los Sistemas de Información a que tengan acceso y recopilar toda la información posible para la detección del problema.

2) Se entiende por incidencia, entre otras:

- a) Cualquier anomalía que afecte al desempeño del puesto de trabajo.
- b) Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.
- c) Cualquier incumplimiento de las Normas Generales de Seguridad.
- d) Cualquier problema que involucre pérdida de información con causa aparente.
- e) Cualquier tipo de intrusión detectada en el sistema.

Procedimientos de gestión de incidencias.

La gestión de incidencias se realizarán a través del siguiente procedimiento:

1) Gestión de incidencias.

4.17) *Criterios de archivo y tratamiento de datos no automatizados.*

El Excmo. Ayuntamiento de Utrera aplica como política de archivo para la documentación en soporte papel unos mínimos necesarios para garantizar plenamente la confidencialidad y el deber de guardar secreto para quien, en virtud de sus competencias, tenga acceso a la información de la entidad.

Con este objetivo general, se establecen las siguientes pautas de conducta en relación al archivo de la documentación, de acuerdo con la Delegación municipal de Cultura:

1) Elementos que constituyen el sistema de archivos del Excmo. Ayuntamiento de Utrera.

* Los archivos de gestión u oficina, que conservan la documentación que generan hasta el final de su tramitación y durante el periodo de vigencia administrativa, que en líneas generales se estima de 3 a 5 años.

* El Archivo General, unidad especializada en las funciones de gestión, conservación (temporal o indefinida), acceso y consulta de los documentos.

Ambos tipos de archivos forman parte del Sistema Archivístico del Excmo. Ayuntamiento de Utrera y responden a las diferentes fases del ciclo de vida de la documentación administrativa. Los documentos de Archivo son los mismos desde que se producen en la oficina hasta que son depositados en un archivo histórico; sin embargo su valor y su función van modificándose en las sucesivas etapas, correspondiendo a cada etapa un tipo de archivo distinto.

FASES DEL CICLO DE VIDA DE LOS DOCUMENTOS			
<i>Fase</i>	<i>Función</i>	<i>Duración</i>	<i>Localización</i>
1) ACTIVA	Documentación en trámite. Vigencia administrativa y consulta frecuente.	3 a 5 años	Archivos de oficina o de gestión
2) SEMIACTIVA	Consulta esporádica. Evaluación para su selección y expurgo.	De 3/6 a 25 años	Archivo Intermedio (integrado en el Archivo General)
3) INACTIVA	Valor histórico y conservación permanente.	A partir de 25 años (valor permanente)	A partir de 25 años (valor permanente)

2) *Expedientes:*

Constituyen la unidad documental básica en todo tipo de archivos.

- Definición: Se entiende por expediente administrativo «una unidad documental formada por un conjunto de documentos generado, orgánica y funcionalmente, por un sujeto productor en la resolución de un mismo asunto».
- Estructura del expediente: debe ser lógica, coherente y cronológica, ordenándose los documentos de acuerdo con el procedimiento o trámite seguido. Los criterios de formación del expediente administrativo deberán ser uniformes y conocidos por todo el personal involucrado en dicha tarea.
- Cada expediente debe estar contenido en una carpetilla o guarda exterior en donde se anotarán todos los datos que identifiquen dicho expediente: nombre de la oficina que lo ha tramitado, fecha de iniciación y finalización, resumen del asunto, nº de documentos, código del cuadro de clasificación con la denominación de la serie y signature de instalación.
- Se aconseja integrar cada documento en su expediente desde el primer momento, ya que transcurrido un tiempo resulta más difícil hacerlo con acierto.
- Se ha de evitar la extracción de documentos originales de los expedientes en tramitación a solicitud de terceros; en este caso se fotocopiarán y devolverán inmediatamente a su lugar.
- Si fuera necesario extraer un documento original de su expediente, además de apuntarlo en un libro de control de préstamos, habrá de quedar en su lugar un testigo (ejem.: hoja tamaño folio de color), haciendo constar el nombre de la persona que se responsabiliza del mismo, la fecha y las indicaciones que permitan identificar tal documento para su posterior recuperación.

3) *Tipos de documentos:*

Los tipos de documentos que forman parte de un expediente administrativo pueden ser:

DOCUMENTOS DE DECISIÓN (Contienen una declaración de voluntad de un órgano administrativo sobre materias de su competencia).	RESOLUCIONES, ACUERDOS, ETC.
DOCUMENTOS DE TRANSMISIÓN (Comunican la existencia de hechos o actos a otras personas, órganos o entidades).	COMUNICACIONES, NOTIFICACIONES, PUBLICACIONES, ETC.
DOCUMENTOS DE CONSTANCIA (Contienen una declaración de conocimiento de un órgano administrativo, cuya finalidad es la acreditación de actos, hechos o efectos).	ACTAS, CERTIFICADOS, CERTIFICACIONES DE ACTO PRESUNTO, ETC.

DOCUMENTOS DE JUICIO (Contienen una declaración de juicio de un órgano administrativo, persona o entidad pública o privada, sobre las cuestiones de hecho o de derecho que sean objeto de un procedimiento administrativo).	INFORMES.
DOCUMENTOS DE LOS CIUDADANOS (El instrumento por el que los ciudadanos se relacionan con la actividad de las Administraciones Públicas).	SOLICITUDES, DENUNCIAS, ALEGACIONES, RECURSOS, ETC.

4) *El Archivo General del Excmo. Ayuntamiento de Utrera:*

El fondo del Archivo General del Excmo. Ayuntamiento de Utrera se forma, principalmente, a partir de las transferencias de los archivos de oficinas de órganos, servicios, secciones, negociados, departamentos, etc. de Institución, siendo imprescindible, por lo tanto, una buena coordinación entre el Archivo General y los archivos de oficinas para trabajar conjuntamente en la consecución de los siguientes objetivos:

* Normalizar los procedimientos de organización de los documentos en las oficinas para facilitar una gestión rápida y eficaz por parte de las unidades administrativas durante el periodo inicial en el que los expedientes se tramitan y custodian en las propias oficinas.

* Establecer las transferencias de las series documentales al Archivo General de forma y manera que los documentos se mantengan organizados y accesibles para la unidades de la Institución y para la sociedad en general, en el contexto en el que se generaron.

* Sentar las bases para el establecimiento de un Sistema que permita la gestión global e integrada de la documentación institucional, independientemente de su soporte físico y de la fase del ciclo de vida en que se encuentre, a partir de los siguientes instrumentos de tratamiento uniforme de los documentos:

- El cuadro de clasificación y codificación de los documentos y los expedientes, de acuerdo con la estructura orgánica y las funciones que se desempeñan en el Ayuntamiento.
- El calendario de conservación y eliminación de los documentos de acuerdo con la normativa del Ayuntamiento de Utrera.
- El sistema de descripción y de gestión, preferiblemente automatizada, de los documentos y expedientes para describir y recuperar la información.

Funciones del Archivo General del Excmo. Ayuntamiento de Utrera

* Recoger, organizar, custodiar y conservar la documentación que le sea remitida por los servicios y unidades administrativas.

* Elaborar los instrumentos para el tratamiento de la documentación, en colaboración con las distintas Unidades y Secciones.

* Gestionar las transferencias documentales de las unidades administrativas.

* Aplicar la evaluación y selección de la documentación, de acuerdo con la normativa establecida por el Ayuntamiento de Utrera.

* Gestionar el préstamo de la documentación a los organismos productores y la consulta de la misma de acuerdo con las normas de acceso a los documentos.

* Proporcionar asesoramiento técnico a los archivos de gestión e impulsar actividades de formación de usuarios.

* Recoger, organizar, custodiar y difundir otros fondos de archivos particulares o institucionales que se incorporen al Ayuntamiento por donación, depósito, compraventa o cualquier otro sistema previsto en el ordenamiento jurídico.

* Facilitar el acceso y difusión del Patrimonio documental del Excmo. Ayuntamiento de Utrera.

5) En aquellos casos en que el Archivo General se encuentre fuera de las dependencias del Ayuntamiento, deberán garantizarse unas medidas de seguridad idénticas a las que existieran en las dependencias centrales del Ayuntamiento.

6) En aquellos casos en que el Archivo General se encuentre fuera de las dependencias del Ayuntamiento y gestionado por una empresa externa, deberá formalizarse por escrito un contrato que regule expresamente el deber de confidencialidad del depositario de la documentación, así como también del resto de obligaciones como encargado del tratamiento.

7) El acceso al archivo deberá encontrarse limitado al horario en que el personal de archivo pueda ejercer los controles previstos. Fuera de este horario, el acceso al archivo estará restringido y controlado. Cualquier acceso al archivo fuera del horario habitual, deberá ser anotado en un registro creado al efecto.

8) El archivo contará con medidas de seguridad físicas apropiadas, protegido con mecanismos que obstaculicen su apertura.

Gestión del archivo y tratamiento de datos no automatizados.

1) Procedimiento de transferencias de documentos al Archivo General.

2) Procedimiento de préstamo de documentos.

4.18) *Gestión de la información no automatizada.*

Es responsabilidad de los empleados y empleadas municipales:

1) Asegurar que toda la documentación en papel con datos de carácter personal se guarde en dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura (llave o similar).

2) Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento el acceso por persona no autorizada, es decir, los documentos que contengan datos de carácter personal solo podrán permanecer sobre la mesa de los/as empleados/as municipales por el tiempo imprescindible necesario para trabajar sobre ellos.

3) Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el párrafo anterior, el Ayuntamiento adoptará las medidas alternativas, debidamente motivadas.

4) Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

5) Todo/a empleado/a, al ausentarse de su puesto de trabajo, debe adoptar las medidas de seguridad adecuadas para que terceros no puedan acceder a la información (cierre de armarios con llaves, control y custodia de las mismas).

FIRMA DE TOMA DE CONOCIMIENTO	
Declaro haber tomado conocimiento de las Directrices Generales de Seguridad y acepto sus obligaciones y las responsabilidades que se deriven de su incumplimiento.	
Nombre y apellidos:	D.N.I.:
Departamento/Servicio:	
Fecha:	
Firma/recibi y conforme:	

5) Organización de la seguridad de la información

5.1) Organización.

Es tal la importancia que adquiere la Seguridad de la Información, por sus implicaciones en los ámbitos legal, político, social, económico, personal, etc., como por su carácter multidisciplinar, basándose en una serie de pilares, humanos, de procedimientos, informáticos, de comunicaciones, etc., y por tener implicaciones en prácticamente todas las áreas del Ayuntamiento, que es necesario que la organización de la Seguridad de la Información se encuentre al máximo nivel.

La multilateralidad de la Seguridad de la Información se acrecienta desde el momento que la Información no solamente se encuentra en soporte mecanizado sino que está disponible en otros, principalmente papel.

Por ello la organización de la Seguridad de la Información se basará en los siguientes órganos de seguridad, que coinciden con órganos concretos del Ayuntamiento:

- a) Comité de Seguridad.
 - b) Responsable de los Ficheros.
 - c) Comité Asesor de Seguridad de la Información.
- Además de estos órganos deben de considerarse los siguientes puestos, unidos a un cargo determinado del organigrama del Ayuntamiento:
- d) Responsable de Seguridad.
 - e) Responsables Internos de los Ficheros (Responsable de Áreas en el Ayuntamiento).
 - f) Encargados del Tratamiento.
 - g) Usuarios.

Quedando estructurada de la siguiente manera:

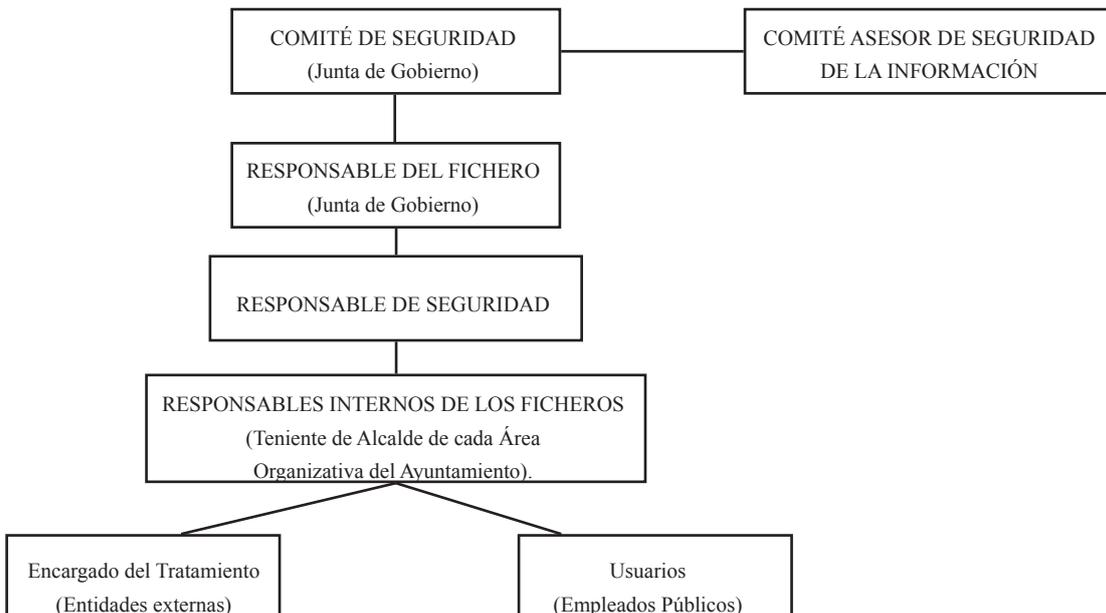


Fig.1: Organigrama de organización de seguridad de la información

5.2) *Comité de Seguridad.*

El Comité de Seguridad será la Junta de Gobierno del Excmo. Ayuntamiento de Utrera. Es el máximo órgano coordinador de las actuaciones que, en materia de Seguridad de la Información, se establecen en el Ayuntamiento.

Las funciones encomendadas al Comité de Seguridad son:

- a) Definir la Política de Seguridad de la Información que debe implantarse en el Ayuntamiento de Utrera.
- b) Aprobar las Directrices Generales de Seguridad de la Información.
- c) Designar al Responsable de Seguridad, cumplimentando con ello el artículo 95 del Reglamento que desarrolla la LOPD, aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre.
- d) Designar el Comité Asesor de Seguridad de la Información.
- e) Aprobar el Documento de Seguridad de la Información Corporativa a propuesta del Responsable de Seguridad.

5.3) *Responsable del Fichero.*

Las responsabilidades sobre la Seguridad de la Información recaen fundamentalmente, según la legislación vigente, en el Responsable del Fichero, identificándose esta figura con la propia Junta de Gobierno, presidida por el Alcalde-Presidente.

De acuerdo con la legislación vigente el Responsable del Fichero, es aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

Dadas las funciones y misiones encomendadas por la LOPD y el Reglamento al Responsable del Fichero, actuará como órgano administrativo, de apoyo del mismo la Secretaría General.

La Junta de Gobierno actuará indistintamente como Comité de Seguridad y como Responsable del Fichero.

De conformidad con la legislación de protección de datos, las tareas asociadas al Responsable de Fichero son:

- a) Notificar, para su inscripción en el Registro General de Protección de Datos, la creación, modificación y cancelación de ficheros que contengan DCPs.
- b) Adoptar las medidas necesarias para que el personal de las unidades usuarias de los Sistemas de Información conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las responsabilidades en que puede incurrir en caso de incumplimiento.
- c) Autorizar el uso de DCPs reales en pruebas en las aplicaciones que manejan los ficheros de los que es responsable y verificar que dichas pruebas se realizan con las medidas de seguridad adecuadas.
- d) Adoptar las medidas correctoras pertinentes para solventar las deficiencias que en materia de seguridad de DCPs se detecten tras la realización de las auditorías de seguridad.
- e) Garantizar la ejecución de los derechos de acceso, modificación y supresión que ejerzan los propietarios de los datos.
- f) Incluir en los formularios, documentos e impresos de recogida de DCPs el texto informativo de tratamiento de datos en ficheros y de ejecución de los derechos de los titulares de los datos.
- g) Incluir en los contratos de prestación de servicios que impliquen acceso a DCPs las cláusulas que establezcan las obligaciones de las empresas de servicios en la seguridad de los datos.
- h) Resolver:
 - h.1) Procedimiento de creación, modificación de ficheros de carácter personal.
 - h.2) Procedimiento de tratamiento de datos por cuenta de terceros.
 - h.3) Procedimiento de transmisión, alojamiento, recepción de información hacia o desde servidores externos al Ayuntamiento.
 - h.4) Procedimiento de autorización de acceso, modificación, cancelación a recursos.
 - h.5) Procedimiento de gestión de cambios de aplicaciones.

NOTA:

* Estas tareas pueden ser delegables en el Responsable de Seguridad.

* Siempre que se exija una autorización, ésta podrá realizarse de forma genérica para un supuesto en abstracto, no siendo necesario realizar autorizaciones concretas para cada vez que se produzca dicho supuesto.

5.4) *Comité Asesor de Seguridad de la Información.*

En este Comité estarán representadas las distintas facetas que pueden distinguirse en la Seguridad de la Información, contemplando los aspectos:

- Legales (Servicios Jurídicos o Delegación Municipal que corresponda).
- Técnicos (Servicio de Informática o Delegación Municipal que corresponda).
- De personal (Servicio de Personal).
- De investigación de faltas o delitos (Servicio de Policía Local).

El Comité Asesor de Seguridad de la Información deberá reunirse periódicamente, al menos cada seis meses para:

- Conocer las modificaciones introducidas en la documentación de seguridad desde la última reunión.
- Adoptar las decisiones que considere adecuadas.
- Asesorar al Responsable de Seguridad de la Información en la realización de las funciones que le encomienda este Documento, y, especialmente, en las cuestiones legales, de personal y de seguridad física.

Asimismo el Comité Asesor de Seguridad de la Información deberá reunirse cuando lo requiera el Responsable de Seguridad.

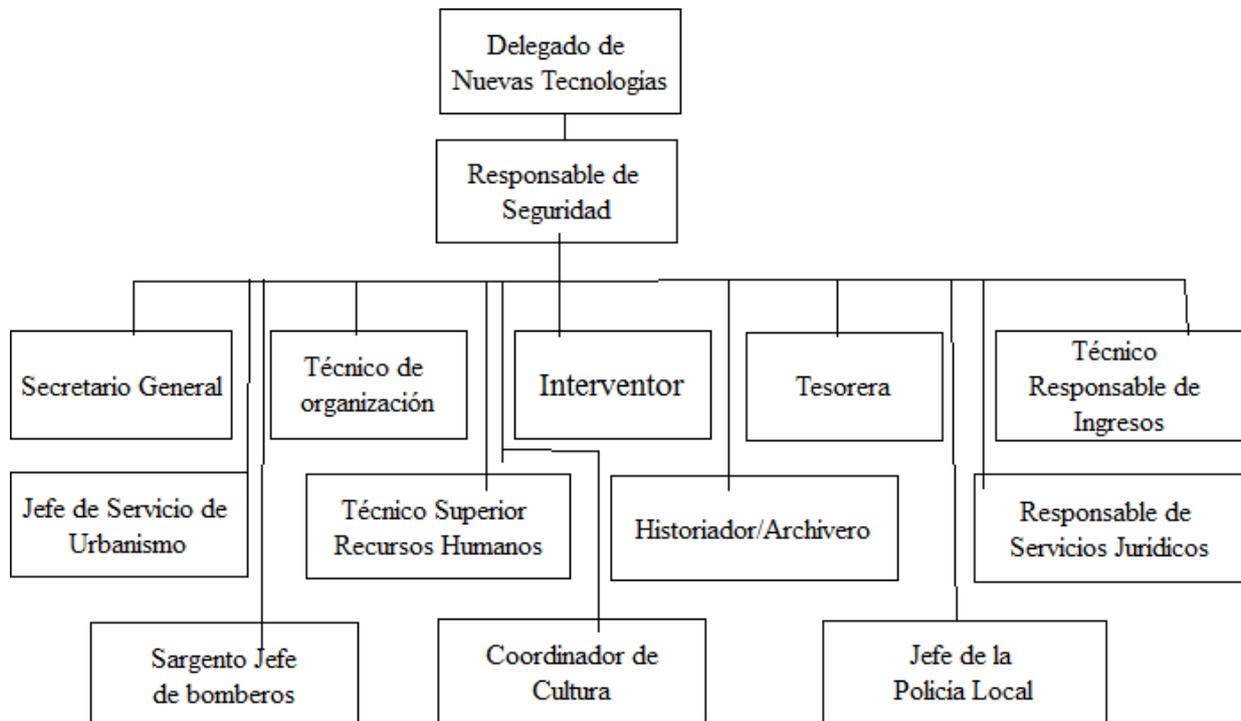


Fig.2: Comité Asesor de la Seguridad de la Información del Excmo. Ayuntamiento de Utrera.

5.5) Responsable de Seguridad.

Esta función debe ser asumida por el Técnico de Informática y comunicaciones o funcionario en quien delegue, cumplimentando con ello el artículo 95 del Reglamento que desarrolla la LOPD aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre.

5.5.1) Funciones de carácter general:

- Aplicar la Política de Seguridad de la Información definida por el Comité de Seguridad.
- Proponer al Comité de Seguridad/Junta de Gobierno las Directrices Generales de Seguridad para su posterior implantación en el Ayuntamiento.
- Estudiar y analizar las posibles estrategias de Seguridad de la Información que pudieran seguirse en el Ayuntamiento.
- Elaborar y modificar en su caso el Documento de Seguridad de la Información para proponerlo a aprobación del Comité de Seguridad/Junta de Gobierno.
- Análisis de las medidas correctoras a implantar, derivadas de los informes de auditoría que se realicen en materia de seguridad de DCPs.
- Revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad de la Información Corporativa que emitan los distintos vocales del Comité.
- Análisis de los informes derivados de las incidencias que afecten de manera grave a los Sistemas de Información.
- Supervisar la ejecución y eficacia de las medidas de seguridad en los distintos servicios municipales.
- Estudiar y en su caso asumir, compromisos sobre protección de datos de carácter personal con otras instituciones públicas o privadas.
- Autorizar por escrito la ejecución de los procesos de recuperación de DCPs, según el procedimiento de Copias de Respaldo y de Recuperación.
- Autorizar las altas, bajas y modificaciones de los accesos de usuarios a las aplicaciones que realizan tratamiento de DCPs.
- Autorizar la salida de soportes informáticos que contengan DCPs fuera de los locales donde se ubica el fichero.

5.5.2) Funciones relacionadas con el Documento de Seguridad de la Información.

Las funciones que tiene que realizar son las siguientes:

- Implantar las medidas y los procedimientos recogidos en el Documento.
- Impulsar las tareas de difusión del mismo.
- Tomar parte activa en la formación del personal.
- Controlar las modificaciones que se produzcan en la estructura de los sistemas informáticos, con objeto de proceder a la actualización del Documento.
- Estar atento a las modificaciones estructurales y organizativas de la entidad, con objeto de proceder a adaptar el Documento a los cambios producidos o previsibles, tendiendo siempre a la prevención.
- Estar al corriente de las nuevas exigencias legales que vayan surgiendo y que pueden repercutir en las medidas de seguridad implantadas en la organización.
- Dar respuesta a las necesidades de protección de información de la organización.
- Informar en los procedimientos administrativos recogidos en el Documento de Seguridad en particular:
 - Procedimiento de creación, modificación de ficheros de carácter personal.

- h.2) Procedimiento de tratamiento de datos por cuenta de terceros
- h.3) Procedimiento de transmisión, alojamiento, recepción de información hacia o desde servidores externos al Ayuntamiento.
- h.4) Procedimiento de autorización de acceso, modificación, cancelación a recursos.
- h.5) Procedimiento de gestión de cambios de aplicaciones.

5.6) *Responsables internos de los ficheros.*

Dentro de las responsabilidades en materia de Seguridad de la Información, adquiere especial importancia la de los Responsables internos de los ficheros, los cuales se corresponden con los Tenientes de Alcalde de cada área organizativa que traten con datos de carácter personal.

Las funciones encomendadas a los Responsables Internos de los Ficheros relativas a la Seguridad de la Información son:

- a) Comunicar al Responsable de Seguridad todas las necesidades de recuperación de datos que se den en el Área de la que es responsable.
- b) Proponer las altas y bajas de acceso de usuarios a su aplicación y/o información correspondiente y velar por el cumplimiento de las normas de seguridad en su entorno de trabajo.
- c) Velar por el cumplimiento de las obligaciones contractuales del Encargado del Tratamiento que corresponda.
- d) Designar, dentro de su Servicio, al responsable de la gestión de soportes con DCPs.

Las tareas asociadas a dicho responsable son:

- * Mantener un inventario actualizado de los soportes que contienen DCPs y registrar las entradas o salidas de los mismos.
- * Supervisar y autorizar la emisión y recepción de soportes que contienen DCPs desde o a otras entidades.
- * Supervisar el cumplimiento de las normas de etiquetado y descontaminación de los soportes con capacidad de almacenamiento y procesamiento.

- e) Autorizar la remisión de información propiedad del Ayuntamiento con destino a otras administraciones, personas físicas y jurídicas para cumplir algunos de los fines del Ayuntamiento y sus contratos.
- f) Dar el visto bueno a las solicitudes relacionadas con datos de carácter personal formuladas por los usuarios del área organizativa a la que correspondan.

5.7) *Encargado del Tratamiento.*

Esta figura es creada para el caso en el que se tenga que contratar con terceros el tratamiento de los datos.

El Encargado del Tratamiento adquiere una responsabilidad contractual con el Ayuntamiento si menoscaba algunas de las normas que se relacionan en el presente Documento.

Sus funciones en lo concerniente a la seguridad de la información, son:

- a) Preservar que solo tengan acceso, y a los ficheros correspondientes, las personas autorizadas para ello, actuando únicamente con el alcance que le haya sido fijado: solo lectura, lectura y copia, modificación, etc.
- b) Comunicar al Responsable del Servicio, cualquier mal funcionamiento de los medios técnicos puestos para regular el control de acceso.
- c) Seguir las instrucciones del Director del Servicio de Informática, en lo que respecta a la configuración de sus accesos, teniendo prohibida la instalación de software o programas no autorizados por aquellos, tengan o no incidencia en el control de accesos.
- d) Hacer cumplir todas las funciones, obligaciones y recomendaciones asignadas a los usuarios de los Sistemas de Información del Ayuntamiento.

Esta figura es creada para el caso en el que se tenga que contratar con terceros el tratamiento de los datos.

El Encargado del Tratamiento adquiere una responsabilidad contractual con el Ayuntamiento si menoscaba algunas de las normas que se relacionan en el presente Documento.

Sus funciones en lo concerniente a la seguridad de la información, son:

- a) Preservar que solo tengan acceso, y a los ficheros correspondientes, las personas autorizadas para ello, actuando únicamente con el alcance que le haya sido fijado: solo lectura, lectura y copia, modificación, etc.
- b) Comunicar al Responsable del Servicio, cualquier mal funcionamiento de los medios técnicos puestos para regular el control de acceso.
- c) Seguir las instrucciones del Director del Servicio de Informática, en lo que respecta a la configuración de sus accesos, teniendo prohibida la instalación de software o programas no autorizados por aquellos, tengan o no incidencia en el control de accesos.
- d) Hacer cumplir todas las funciones, obligaciones y recomendaciones asignadas a los usuarios de los Sistemas de Información del Ayuntamiento.

6) *Clasificación de la información*

Entendiéndose por «Información Personal» todos los ficheros, en cualquier tipo de soporte, afectados por la Ley Orgánica de Protección de Datos. Los ficheros con datos de carácter personal se clasifican según el TÍTULO VIII del Reglamento 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 81 dice:

1.—Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2.—Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

- a) Los relativos a la comisión de infracciones administrativas o penales.
- b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

- c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- d) Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- e) Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- f) 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.

3.—Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

- a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- c) Aquellos que contengan datos derivados de actos de violencia de género.

4.—A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5.—En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- a) 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.
- b) Se trate de ficheros o tratamientos en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad. Letra b) del número 5 del artículo 81 redactada por la disposición adicional cuarta del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica («B.O.E.» 29 enero). Vigencia: 30 enero 2010.

6.—También podrán implantarse las medidas de seguridad de nivel básico en 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.

7.—Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8.—A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

7) *Ficheros con Datos de Carácter Personal.*

En este apartado se recogen los ficheros con Datos de Carácter Personal existentes en el Ayuntamiento, relacionados por niveles. La estructura de éstos es la siguiente:

- a) Finalidad del fichero y los usos previstos para el mismo.
- b) Personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos.
- c) Procedimiento de recogida de datos.
- d) Procedencia de los datos.
- e) Estructura básica del fichero y descripción de los tipos de datos.
- f) Cesiones de datos de carácter personal.
- g) Responsable del Fichero.
- h) Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- i) Nivel de seguridad LOPD.
- j) Disposiciones.
- k) Observaciones.

La estructura de cada uno de los ficheros se presenta en el anexo nº 1, ordenados por el nivel de seguridad LOPD de los mismos.

* Ficheros de nivel BAJO.

* Ficheros de nivel MEDIO.

* Ficheros de nivel ALTO.

8) *Procedimientos.*

Los procedimientos de seguridad a aplicar en el funcionamiento diario del Ayuntamiento se describen brevemente todos y cada uno de ellos seguidamente:

PR001	<p>Procedimiento de creación, modificación de ficheros de carácter personal.</p> <p>Tiene por objeto la creación y modificación de ficheros que en todo caso deberá estar conforme al Título V del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.</p>
PR002	<p><i>Procedimiento de acceso, modificación, cancelación de datos de carácter personal.</i></p> <p>Conforme a lo dispuesto en la LOPD, el RLPD, las personas pueden ejercer los derechos de acceso, rectificación, cancelación y oposición respecto de los datos que obren en poder de las Administraciones públicas. Dichos derechos deberán poderse ejercer mediante el procedimiento de referencia indicado en el artículo 25 del Título III del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.</p>
PR003	<p><i>Procedimiento para tratamiento de datos por cuenta de terceros.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero, así como informe del Responsable de Seguridad que previo análisis de los riesgos comprobará:</p> <ul style="list-style-type: none"> i) La inexistencia de trabas legales para ello. ii) Verificará la suscripción de contrato o convenio expreso entre el Ayuntamiento de Utrera y la empresa responsable de la prestación del servicio. iii) El cumplimiento por parte de la empresa responsable de lo previsto en el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad. iv) El cumplimiento de lo previsto en la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. v) El acuerdo de confidencialidad y de nivel de servicio que procedan. vi) El seguimiento de la Guía CCN-STIC-823 del Centro Criptológico Nacional <p>El informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de la solicitud.</p>
PR004	<p><i>Procedimiento para transmitir, alojar y/o recepcionar información hacia/desde servidores externos al Ayuntamiento.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero, así como informe del Responsable de Seguridad que previo análisis de los riesgos comprobará:</p> <ul style="list-style-type: none"> i) La inexistencia de trabas legales para ello. ii) Verificará la suscripción de contrato o convenio expreso entre el Ayuntamiento de Utrera y la empresa responsable de la prestación del servicio. iii) El cumplimiento por parte de la empresa responsable de lo previsto en el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad. iv) El cumplimiento de lo previsto en la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal. v) El acuerdo de confidencialidad y de nivel de servicio que procedan. vi) El seguimiento de la Guía CCN-STIC-823 del Centro Criptológico Nacional <p>El informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de la solicitud.</p>
PR005	<p><i>Procedimiento para la autorización de actualización de la información contenida en las bases de datos municipales desde fuera de las aplicaciones internas del Ayuntamiento de Utrera.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero. Requiere la emisión de informe del Responsable de Seguridad y la resolución de la solicitud por el Responsable del Fichero.</p>
PR006	<p><i>Procedimiento para el respaldo y/o recuperación de datos, ficheros y servicios de las copias de seguridad.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero. La delegación de Nuevas Tecnologías dejará constancia de la recuperación en el registro correspondiente. Se debe dar traslado periódicamente al Responsable del Fichero para su conocimiento.</p>
PR007	<p><i>Procedimiento de autorización de acceso, modificación, cancelación a recursos.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero. Requiere la emisión de informe del Responsable de Seguridad y la resolución de la solicitud por el Responsable del Fichero.</p>
PR008	<p><i>Procedimiento de control de acceso a aplicaciones y sistemas.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el Responsable del Departamento donde el empleado realice su actividad y el visto bueno del Responsable interno del fichero.</p> <p>Si el empleado para el que se pide un acceso a aplicaciones, ha cambiado su situación dentro del Ayuntamiento, deberá constar en el expediente, el resultado del procedimiento de gestión de usuarios, altas, modificaciones y bajas.</p> <p>Requiere informe del Responsable de Seguridad.</p> <p>Del informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de acceder a lo solicitado.</p>

PR009	<p><i>Procedimiento de gestión de usuarios; altas, modificaciones y bajas.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el Responsable del Departamento de RRHH, y el visto bueno del Concejal-Delegado de Recursos Humanos.</p> <p>También debe constar en el expediente</p> <p>Requiere informe del Responsable de Seguridad.</p> <p>Del informe se dará traslado al Responsable del Fichero quién decidirá sobre la procedencia o no de acceder a lo solicitado.</p>
PR010	<p><i>Procedimiento de asignación, distribución y almacenamiento de contraseñas.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado.</p>
PR011	<p><i>Procedimiento de gestión de incidencias.</i></p> <p>Las incidencias podrán comunicarse a través de la aplicación dedicada al efecto o bien telefónicamente debiendo la Delegación de Nuevas Tecnologías dejar constancia de la incidencia y de la persona que la comunica.</p>
PR012	<p><i>Procedimiento de remisión de información propiedad del Ayuntamiento.</i></p> <p>Se deberá usar el PROCEDIMIENTO PARA TRANSMITIR, ALOJAR O RECEPCIONAR INFORMACIÓN HACIA O DESDE SERVIDORES EXTERNOS AL AYUNTAMIENTO para tener autorizado por norma general de la remisión de una tipología concreta de información. Una vez autorizada que la información referida se puede remitir habitualmente a otras administraciones, personas físicas o jurídicas para cumplir alguno de los fines del Ayuntamiento y sus contratos deberá quedar materializada en el Registro de Salida del Ayuntamiento de Utrera previa autorización del Responsable Interno del Fichero.</p>
PR013	<p><i>Procedimiento de acceso excepcional a los datos para otro empleado municipal.</i></p> <p>En todo caso habrá de constar en el expediente administrativo solicitud firmada por el interesado con el visto bueno del Responsable interno del fichero. Requiere la emisión de informe del Responsable de Seguridad y la resolución de la solicitud por el Responsable del Fichero.</p>
PR014	<p><i>Procedimiento de gestión de cambios de aplicaciones.</i></p> <p>En todo caso deberá constar en el expediente solicitud del interesado con el visto bueno del Responsable Interno del Fichero seguido del informe correspondiente del Responsable de Seguridad e informe del técnico que corresponda en el que debe constar:</p> <ul style="list-style-type: none"> * La aplicación del Título IV del Reglamento Regulador de la Administración Electrónica del Ayuntamiento de Utrera a los cambios/mejoras funcionales solicitados. * La aplicación de la normativa vigente en materia de Administración Electrónica y su normativa de desarrollo.
PR015	<p><i>Procedimiento de gestión de la configuración de aplicaciones.</i></p> <p>En todo caso deberá constar en el expediente solicitud del interesado con el visto bueno del Responsable Interno del Fichero.</p>
PR016	<p><i>Procedimiento de control de accesos.</i></p> <p>Tiene por objeto describir las actuaciones que deberá llevar a cabo el personal responsable de garantizar que sólo puedan acceder a los sistemas y aplicaciones los usuarios debidamente autorizados, con los permisos que a cada uno correspondan una vez que hayan sido dados de alta.</p>
PR017	<p><i>Procedimiento de control de acceso físico.</i></p> <p>Tiene por objeto describir las acciones a realizar por el personal responsable de accesos a los edificios, al Servicio de Informática y a los Centros de Procesos de Datos (CPDs) para impedir intrusiones no deseadas y evitar que se conozca la ubicación de los CPDs.</p>
PR018	<p><i>Procedimiento de control de servidores.</i></p> <p>Tiene por objeto garantizar que los equipos centrales en que residen las aplicaciones y bases de datos corporativas se mantienen en condiciones adecuadas para garantizar la disponibilidad del servicio.</p>

PR019	<p><i>Procedimiento de transferencias de documentos al archivo general</i></p> <p>1º) El primer paso es ponerse en contacto con el Archivo General para acordar las fechas de traslado y aclarar dudas respecto a la forma de enviar la documentación.</p> <p>ARCHIVO GENERAL DEL EXCMO. AYUNTAMIENTO DE UTRERA</p> <p>Plaza de Gibaxa, 1. Teléfono: 95 486 00 50 - Ext.: 220 e-mail: jmena@utrera.org</p> <p>Es aconsejable que la Unidad Administrativa cumplimente el formulario:</p> <p>Hoja de previsión de transferencia de documentos. (Anexo I), cuyo modelo se puede obtener en el portal del empleado. De esta forma, el Archivo General puede conocer de antemano el volumen y características de la documentación a transferir, planificar los flujos de trabajo del Archivo y ponerse en contacto con la Unidad correspondiente para aclarar cualquier cuestión al respecto.</p> <p>La documentación objeto de transferencia deberá estar organizada. El responsable del archivo de gestión se encargará de preparar la documentación para remitirla al Archivo General, bajo la supervisión del Jefe del Servicio o Unidad y con el asesoramiento técnico del Archivo General siempre que sea necesario.</p> <p>2º) Preparación de los documentos a transferir:</p> <p>- a) Revisar los documentos:</p> <ul style="list-style-type: none">- Antes de guardar los documentos en las cajas de archivo, se comprobará que no falta ningún documento dentro de los expedientes o expedientes dentro de la serie documental.- Verificar la ordenación correcta (numérica, cronológica o alfabética...) de los documentos.- Separar, si no se ha hecho con anterioridad, todas las copias, duplicados, borradores... y todos los documentos que no estén relacionados directamente con el asunto o actividad para el cual se ha constituido el expediente.- Los expedientes deben estar libres de clips, grapas, gomas, carpetas de plástico o cualquier otro elemento que pudiese afectar a su conservación. Las carpetas colgantes serán sustituidas por carpetas de cartulina y las carpetas de anillas (A-Z) por cajas de archivo normalizadas. <p>b) Agrupar los documentos en expedientes de acuerdo con la ordenación de los asuntos o actividades a los cuales se refieren.</p> <p>En el caso de que se considere imprescindible mantener unidos varios documentos en el interior del expediente se pueden utilizar subcarpetas de hojas de DIN-A3.</p> <p>c) Colocar los expedientes en carpetas de cartulina proporcionadas por el Archivo o bien en las carpetas normalizadas con el logotipo del Excmo. Ayuntamiento de Utrera, en cuya cubierta se anotará la descripción del expediente mediante etiqueta adhesiva según el modelo propuesto por el Archivo General (Anexo II), en el que se harán constar los siguientes datos:</p> <ul style="list-style-type: none">- Nombre del órgano o de la unidad administrativa (Servicio, Sección, Negociado...).- La denominación propia de la serie documental que se transfiere y código de clasificación correspondiente.- Las fechas extremas de los documentos que contiene el expediente.- Número de volumen, cuando un expediente por su extensión ocupe más de una carpeta. <p>Asimismo, se puede hacer constar otra información de interés para la oficina, tal como:</p> <ul style="list-style-type: none">- Título del expediente (para identificarlo entre los expedientes de la misma naturaleza o serie).- La signatura o número de referencia que tenga en la Unidad Administrativa de origen.
-------	---

PR019	<p>d) Colocar las carpetas en cajas:</p> <ul style="list-style-type: none"> - Las carpetas con los expedientes se guardarán en cajas archivadoras de cartón de archivo definitivo de tamaño folio (el Archivo General las puede proporcionar a petición de las oficinas), que deberán llenarse sin llegar a estar apretadas, evitando dejar cajas semivacías. - Los expedientes se guardarán de forma ordenada siguiendo un orden ascendente y cronológico en cajas correlativas, según un orden de mayor a menor edad. - El Archivo General no admitirá documentación suelta ni guardada en contenedores que no sean las cajas normalizadas. - En los casos de documentación que, por su tamaño o características, no pueda ser introducida en las cajas normalizadas, se utilizará el formato más conveniente, de acuerdo con el Archivo General. <p>e) Rotulación de las cajas:</p> <ul style="list-style-type: none"> - Para identificar cada caja se podrán utilizar los tejuelos proporcionados por el Archivo General (Anexo III), en los que se podrán cumplimentar los siguientes datos: <ul style="list-style-type: none"> o Número de identificación de la caja dentro de la transferencia, a lápiz. Esta numeración será correlativa y se corresponderá con el número asignado en la Hoja de transferencia de documentos, procedimiento que se describe en el siguiente apartado. o Unidad /Centro o Servicio o Nombre de la serie documental que contiene. o Año/s: primera y última fecha de la documentación contenida en la caja. - No es obligatorio el uso de los tejuelos por parte de las oficinas, si bien sí que es imprescindible que las Oficinas anoten a lápiz en el lomo de las cajas la numeración correlativa de las cajas que se transfieren, con objeto de que el Archivo pueda identificarlas dentro de la transferencia y cotejar el contenido de las mismas con los datos cumplimentados en la Hoja de transferencia. <p>f) Redacción de la hoja de transferencia de documentos:</p> <ul style="list-style-type: none"> - El responsable del Archivo de oficina cumplimentará tres copias de la Hoja de transferencia de documentos (Anexo IV), cuyo modelo está disponible en el Portal del Empleado. Dos copias se enviarán al Archivo y la tercera quedará en poder de la oficina correspondiente para su control e información interna. - Este documento cumple una doble función: <ul style="list-style-type: none"> o Es el elemento que prueba el traspaso de documentación que se va a efectuar. o Facilita el control y la localización de los documentos, tanto para el Archivo General como para la Unidad Administrativa remitente. - En la Hoja de transferencia de documentos, la oficina remitente hará constar los siguientes datos: <p>Datos de la cabecera:</p> <ul style="list-style-type: none"> o Nombre del órgano remitente. o Nombre, teléfono y dirección de correo electrónico del responsable del archivo de gestión. o Fecha de la transferencia. o Número total de cajas de archivo que se transfieren. o Nº de transferencia: este dato no se cumplimenta, ya que será asignado por el Archivo. <p>Descripción:</p> <ul style="list-style-type: none"> o Número de orden de cada una de las cajas que componen la transferencia. (El último número ha de coincidir con el nº total de cajas de la transferencia). o Denominación de la serie y contenido específico de cada caja. o Fechas extremas (Primera y última de los documentos contenidos en cada caja). o Periodo de vigencia administrativa. o Signatura en el Archivo: Este dato será cumplimentado en el Archivo General cuando se le asigne el número definitivo en el depósito y se hará constar en la copia que el Archivo devolverá a la oficina para facilitar futuras consultas por parte de la misma. <p>Sello del órgano remitente y firma del responsable de dicha Unidad.</p> <p>3º) Formalización de la transferencia.</p> <ul style="list-style-type: none"> - Una vez que la transferencia esté preparada, se concretará con el Archivo General la fecha de traslado. - El traslado de los fondos documentales al Archivo General es responsabilidad e irá a cargo del organismo remitente. <p>4º) El Archivo General realizará a continuación las siguientes tareas:</p> <ul style="list-style-type: none"> o Comprobar la conformidad entre lo reseñado en la hoja de transferencia y la documentación recibida. En el supuesto de que no haya coincidencia, la hoja será devuelta a su remitente para subsanar los errores detectados. o Devolver a la oficina correspondiente un ejemplar de la hoja de transferencia, firmada y sellada por el Archivo General, como confirmación de que la transferencia ha sido realizada, en la que se incluirá la signatura topográfica que se le haya adjudicado en el Archivo. o Esta signatura será utilizada como referencia siempre que se solicite una consulta o préstamo de documentación al Archivo General. o Las copias de las hojas de transferencia han de ser guardadas y ordenadas por el Organismo remitente y conocidas por su personal.
-------	--

PR020	<p><i>Procedimiento de préstamo de documentos</i></p> <p>1) La unidad administrativa del Excmo. Ayuntamiento de Utrera que desee solicitar un préstamo de documentación al Archivo General, debe hacer uso del formulario de solicitud de préstamo el Portal del Empleado, imprimirlo, cumplimentarlo, y enviarlo al Archivo, firmado por el responsable de la unidad administrativa. Este formulario refleja el procedimiento de préstamo y ha de acompañar a la documentación en todas las fases del procedimiento.</p> <p>2) Si una unidad administrativa solicita un préstamo de documentación con valor administrativo de la que no ha sido productora, debe dirigir la petición a la unidad administrativa responsable del procedimiento.</p> <p>3) El formulario de solicitud de préstamo incluye los siguientes campos:</p> <ul style="list-style-type: none">• Nombre del solicitante.• Unidad administrativa.• Nombre del responsable que solicita.• Correo electrónico y teléfono del solicitante.• Fecha de la solicitud.• Datos de la documentación:<ul style="list-style-type: none">- Descripción (título de la serie y del expediente que se requiere).- Años.- Signatura de la documentación en el Archivo General.- Observaciones que la unidad administrativa solicitante quiera.- Añadir en relación a las características de la documentación que solicita, plazos especiales, motivo de la solicitud, etc.• Datos de control interno del préstamo (los cumplimenta el Archivo General):<ul style="list-style-type: none">- Número de préstamo.- Fecha de devolución.- Fecha de devolución en caso de prórroga.• Firmas, sellos y fechas del procedimiento administrativo del préstamo:<ul style="list-style-type: none">- Firma (con fecha y sello) del responsable de la unidad administrativa solicitando el préstamo.- Firma (con fecha y sello) del responsable del Archivo dando curso al préstamo.- Firma (con fecha y sello) del responsable de la unidad administrativa devolviendo el préstamo.- Firma (con fecha y sello) del responsable del Archivo acusando recibo de la documentación devuelta. <p>4) Una vez que el Archivo General recibe el formulario, se prepara la documentación solicitada y se remite a la unidad administrativa peticionaria, acompañada por el formulario en donde el Archivo ha consignado los datos de número de préstamo, fecha de devolución y ha firmado y fechado el envío del préstamo.</p> <p>5) Dentro del plazo de préstamo establecido (un mes), la unidad administrativa devuelve la documentación al Archivo General, junto con el formulario en donde ha fechado, firmado y sellado la devolución.</p> <p>6) Si la unidad administrativa tiene razones para mantener el préstamo durante un plazo más amplio del establecido, es necesario que solicite una prórroga al Archivo General.</p> <p>7) La documentación se devuelve al Archivo General sin modificaciones. Si fuera necesario añadir al expediente algún documento, el responsable de la unidad administrativa lo hará constar en la portada de la carpeta correspondiente y advertirá de ello al Archivo General.</p> <p>8) En caso de pérdida o deterioro de la documentación, la responsabilidad recae en la persona de la unidad administrativa solicitante del préstamo.</p> <p>9) Una vez recibida la documentación prestada, el Archivo General remite al prestatario el formulario con el acuse de recibo fechado, firmado y sellado.</p>
-------	---

9) *Cláusulas a incluir en documentos.*

1 - CLÁUSULA A INCLUIR EN LOS FORMULARIOS DE RECOGIDA DE DATOS DE CARÁCTER PERSONAL

(A incluir en todo tipo de instancias, solicitudes, comparecencias, declaraciones, etc. de los interesados).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al interesado de que sus datos personales van a ser incorporados para su tratamiento a los correspondientes ficheros municipales. La recogida y tratamiento de dichos datos tiene como finalidad proceder a la tramitación de de la solicitud realizada, la comunicación y notificación de cualquier actuación administrativa, así como la formación y mantenimiento de ficheros acreditativos de las distintas relaciones jurídico-administrativas de las que pueda Vd. ser titular en este Ayuntamiento. Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

2 - CLÁUSULA A INCLUIR EN LOS FORMULARIOS DE RECOGIDA DE DATOS DE CARÁCTER PERSONAL

(Si el formulario a rellenar por el interesado tiene la forma de cuestionario-encuesta, es necesario indicar qué preguntas son de carácter obligatorio o si son de carácter voluntario).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al interesado de que sus datos personales van a ser incorporados para su tratamiento a los correspondientes ficheros municipales. La recogida y tratamiento de dichos datos tiene como finalidad _____ (insertar la finalidad que corresponda). La cumplimentación de todos los datos que se solicitan es de carácter obligatorio, excepto las preguntas __ , __ y __ que son de carácter voluntario. Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

3 - CLÁUSULA A INCLUIR EN LOS FORMULARIOS DE RECOGIDA DE DATOS DE CARÁCTER PERSONAL

(Si los datos de carácter personal van a ser cedidos, se deberá informar de forma previa de dicha cesión al titular de los datos).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al interesado de que sus datos personales van a ser incorporados para su tratamiento a los correspondientes ficheros municipales. La recogida y tratamiento de dichos datos tiene como finalidad _____ (insertar la finalidad que corresponda). El/La interesado/a autoriza al Excmo. Ayuntamiento de Utrera para ceder sus datos personales desde este mismo momento para su utilización en las finalidades expuestas a _____ (insertar la denominación de la empresa o entidad a la que se cederán los datos). Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

4 - CLÁUSULAS INFORMATIVAS EN RELACIÓN AL PERSONAL

(Nota interior o circular a enviar a todos los empleados actuales).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al empleado municipal de que sus datos personales están siendo tratados de manera automatizada y no automatizada con la finalidad de llevar a cabo el adecuado desarrollo, cumplimiento y control de la relación profesional existente en la actualidad. La información personal recabada de los empleados municipales está almacenada en los ficheros de los que es responsable este Excmo. Ayuntamiento de Utrera, que asume las medidas de índole técnica, organizativa y de seguridad que garanticen la confidencialidad e integridad de la información, de acuerdo con lo establecido en el Real Decreto 1720/2007 de 21 de Diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, así como lo dispuesto en la propia Ley Orgánica y en la Ordenanza Reguladora de la Seguridad de la Información, Creación, Modificación y Supresión de los ficheros de carácter personal del Excmo. Ayuntamiento de Utrera.

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

5 - CLÁUSULAS INFORMATIVAS EN RELACIÓN AL PERSONAL

(Cláusula a incluir en los contratos laborales).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, el/la trabajadora autoriza el tratamiento de sus datos personales recogidos en este contrato y durante el proceso de incorporación, todos ellos necesarios para la prestación de servicios de gestión vinculados a la relación laboral, así como para otros servicios relacionados con su carrera profesional y con el Departamento de Recursos Humanos del Excmo. Ayuntamiento de Utrera.

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

6 - CLÁUSULAS INFORMATIVAS EN RELACIÓN AL PERSONAL

(Cláusula a incluir en el nombramiento de funcionarios).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, el/la funcionario/a autoriza el tratamiento de sus datos personales recogidos en este nombramiento, todos ellos necesarios para ejercer sus funciones, así como para otros servicios relacionados con su carrera profesional y con el Departamento de Recursos Humanos del Excmo. Ayuntamiento de Utrera.

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

7 - CLÁUSULAS INFORMATIVAS EN RELACIÓN CON LOS PROVEEDORES

(Cláusula para incorporar a las facturas y/o pedidos y/o contratos con los proveedores).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, el Excmo. Ayuntamiento de Utrera le informa que sus datos personales aportados en este _____ (indicar si es contrato, pedido, factura, etc.), serán incorporados a un fichero de datos de carácter personal titularidad del Excmo. Ayuntamiento de Utrera, con la finalidad de gestionar la relación negocial entre éste y sus proveedores.

El proveedor autoriza el tratamiento de sus datos personales recogidos en este documento, necesarios para la prestación de servicios de gestión vinculados a la relación negocial con este Excmo. Ayuntamiento.

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

8 - CLÁUSULA INFORMATIVA EN RELACIÓN CON LOS PROVEEDORES

(Cláusula o circular a enviar a todos los proveedores actuales).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al proveedor de que sus datos personales están siendo tratados de manera automatizada y no automatizada con la finalidad de llevar a cabo el adecuado desarrollo, cumplimiento y control de la relación negocial existente en la actualidad.

La información personal recabada de los proveedores está almacenada en los ficheros de los que es responsable este Excmo. Ayuntamiento de Utrera, que asume las medidas de índole técnica, organizativa y de seguridad que garanticen la confidencialidad e integridad de la información, de acuerdo con lo establecido en el Real Decreto 1720/2007 de 21 de Diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, así como lo dispuesto en la propia Ley Orgánica y en la Ordenanza Reguladora de la Seguridad de la Información, Creación, Modificación y Supresión de los ficheros de carácter personal del Excmo. Ayuntamiento de Utrera.

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

9 - CLÁUSULA INFORMATIVA A INCORPORAR EN LOS FICHEROS CUYOS DATOS NO SE OBTIENEN DIRECTAMENTE DEL PROPIO INTERESADO.

(Cláusula informativa a incorporar en los ficheros cuyos datos no se obtienen directamente del propio interesado o su representante legal, sino que proceden de otras vías: otras personas físicas, fuentes accesibles al público, registros públicos, administraciones públicas o entidades privadas).

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, el Excmo. Ayuntamiento de Utrera le informa que sus datos personales han sido incluidos en un fichero propiedad de este Excmo. Ayuntamiento, con la finalidad de _____ (insertar la finalidad que corresponda).

Sus datos personales proceden de _____ (insertar la fuente accesible al público de donde han sido extraídos).

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

10 - DERECHO A LA INFORMACIÓN A TRAVÉS DE CORREO ELECTRÓNICO, CARTA O CORREO ORDINARIO.

(Cláusula informativa a incorporar en los ficheros cuyos datos no se obtienen a través de correo electrónico, carta o correo ordinario).

Cuando se recojan datos a través del correo electrónico, carta o correo ordinario, la forma de cumplir con el derecho de información será responder al mismo con otro en el que se recojan los aspectos del artículo 5 de la LOPD, conforme a las cláusula número 1 expuesta anteriormente.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al interesado de que sus datos personales van a ser incorporados para su tratamiento a los correspondientes ficheros municipales. La recogida y tratamiento de dichos datos tiene como finalidad proceder a la tramitación de de la solicitud realizada, la comunicación y notificación de cualquier actuación administrativa, así como la formación y mantenimiento de ficheros acreditativos de las distintas relaciones jurídico-administrativas de las que pueda Vd. ser titular en este Ayuntamiento. Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

11 - DERECHO A LA INFORMACIÓN A TRAVÉS DE ENTREVISTAS PERSONALES O POR VÍA TELEFÓNICA.

Cuando se recojan datos mediante entrevistas personales o por vía telefónica, se informará de los aspectos del artículo 5 de la LOPD, de forma oral o bien en un panel situado en un lugar visible del local donde se realice la recogida de datos.

Además de lo anteriormente expuesto, aprovechando la primera comunicación escrita con el interesado, se realizará un recordatorio conforme a la cláusula número 1 de las anteriores.

En cualquier caso, la mejor solución -siempre que sea viable- será sustituir los anteriores medios de recogida de datos por el de un formulario, ya sea en papel o en la web municipal, donde se incluirá la cláusula número 1 de las anteriores.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se informa al interesado de que sus datos personales van a ser incorporados para su tratamiento a los correspondientes ficheros municipales. La recogida y tratamiento de dichos datos tiene como finalidad proceder a la tramitación de de la solicitud realizada, la comunicación y notificación de cualquier actuación administrativa, así como la formación y mantenimiento de ficheros acreditativos de las distintas relaciones jurídico-administrativas de las que pueda Vd. ser titular en este Ayuntamiento. Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

Si lo desea, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición en los términos establecidos en la legislación vigente, mediante escrito dirigido a la Junta de Gobierno Local de este Excmo. Ayuntamiento, Plaza de Gibaxa, 1 - 41710 - Utrera (Sevilla).

12 - CLAUSULA DE CONFIDENCIALIDAD A INTRODUCIR EN TODOS LOS CONTRATOS O CONVENIOS QUE CELEBRE ESTE EXMO. AYUNTAMIENTO.

1) _____ (a) _____ se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará Información confidencial cualquier dato al que _____ (a) _____ acceda en virtud de las relaciones referenciadas en el _____ (b) _____, en especial la información y datos propios del Ayuntamiento de Utrera a los que haya accedido durante la ejecución de la prestación de servicio objeto del _____ (c) _____.

_____ (a) _____ se compromete a no divulgar dicha Información confidencial, así como a no publicarla ni de cualquier otro modo, bien directamente, bien a través de terceras personas o empresas ni ponerla a disposición de terceros sin el previo consentimiento por escrito del Ayuntamiento de Utrera.

2) De igual modo, _____ (a) _____, se compromete, tras la extinción de las citadas relaciones, a no conservar copia alguna de información confidencial.

3) _____ (a) _____, informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en el presente documento sobre confidencialidad, así como de las obligaciones relativas al tratamiento automatizado de datos de carácter personal. _____ (a) _____, realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios con su personal y colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones.

4. _____ (a) _____ reconoce que la legislación sobre Protección de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre; Real Decreto 1720/2007, de 21 de Diciembre por el que se aprueba el desarrollo de la citada Ley; y artículos 197 y 278 del Código Penal) establece una serie de obligaciones en el tratamiento de datos de carácter personal aplicables a los encargados del tratamiento. A tal efecto, _____ (a) _____:

a) Únicamente accederá a los datos personales de usuarios del servicio y demás personas físicas relacionadas con el Ayuntamiento de Utrera si tal acceso fuese necesario para cumplir con las obligaciones establecidas para _____ (a) _____, en el presente _____ (c) _____.

b) Se compromete a:

* Utilizar los datos de carácter personal a los que tenga acceso única y exclusivamente para cumplir con sus obligaciones contractuales/conveniales derivadas de los servicios prestados para el Ayuntamiento de Utrera.

* Observar y adoptar cuantas medidas de seguridad sean necesarias para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso, y en especial, las que le sean notificadas por el Ayuntamiento de Utrera, así como adoptar en el futuro cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, la confidencialidad e integridad en el tratamiento automatizado o no de datos personales.

* A no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.

* A destruir los datos cedidos por el Ayuntamiento de Utrera una vez finalizada la vigencia de las relaciones entre ambas partes, salvo que el Ayuntamiento de Utrera autorice a su conservación de forma expresa y por escrito, si las partes prevén la ejecución de nuevos servicios que impliquen de forma necesaria el acceso a datos personales del Ayuntamiento de Utrera por parte de _____ (a) _____.

5) Las obligaciones establecidas para _____ (a) _____ en la presente cláusula serán también de obligado cumplimiento para sus empleados, colaboradores, tanto externos como internos, y subcontratistas, por lo que _____ (a) _____, responderá frente al Ayuntamiento de Utrera si tales obligaciones son incumplidas por tales empleados, colaboradores o subcontratistas.

6) El incumplimiento por parte de _____ (a) _____, de cualesquiera de las obligaciones establecidas en la presente cláusula, generará una indemnización en favor del Ayuntamiento de Utrera en la cuantía de las sanciones que por infracciones graves o muy graves señala la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de diciembre, más la correspondiente indemnización por los daños y perjuicios ocasionados.

7) Las obligaciones de confidencialidad establecidas en el presente documento tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre _____ (a) _____ y el Ayuntamiento de Utrera.

(a) Indicar el nombre y apellidos o la razón social del contratista o la entidad que formaliza el convenio con el Ayuntamiento.

(b) Indicar el contrato o convenio de colaboración con indicación de su objeto.

(c) Contrato ó convenio.

En Utrera a 20 de febrero de 2014.—El Secretario General, Juan Borrego López.