AYUNTAMIENTO DE OSUNA

DECRETO DE ALCALDÍA.

Considerando que por Decreto de la Alcaldía número 2021-0482, de 29 abril de 2021 se crea y asignaron funciones al Comité de Seguridad de la Información del Ayuntamiento de Osuna.

Considerando que este Ayuntamiento se encuentra inmerso en el proceso de adaptación, tanto al Reglamento General de Protección de Datos Europeo y normativa estatal vigente en dicha materia, como al Esquema Nacional de Seguridad.

Considerando la necesidad de aprobación de un documento de organización interna establecida en el art. 15 del Esquema Nacional de Seguridad:

"1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Considerando al imperativo legal que impulsa la redacción de esta normativa, y es lo dispuesto en el art. 87.3 de la Ley Orgánica de Protección de Datos, 3/2018 de 5 de diciembre:
"Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado."

En virtud de las potestades atribuidas por el art. 21 de la Ley 7/85, Reguladora de las Bases de Régimen Local, ACUERDO:

PRIMERO.- Aprobar el documento que se anexa a esta resolución, referente a la Normativa para el cumplimiento y uso seguro de la información y servicios del Ayuntamiento de Osuna.

SEGUNDO.- Publicar dicha Normativa para el cumplimiento y uso seguro de la información y servicios del Ayuntamiento de Osuna en el Tablón de Anuncios Municipal, en el Portal de Transparencia y difundir entre los empleados públicos municipales para su conocimiento y actamiento.

LA ALCALDESA-PRESIDENTA LA SECRETARIA GENERAL

ROSARIO ANDUAR TORREJON (1 de 2)
ALCALDESA
Fecha Firma: 19/01/2024
HASH: fc6eeab98f67743e1a51307a8ad3d052

SARA BELEN TROYA JIMENEZ (2 de 2)
SECRETARIA GENERAL
Fecha Firma: 19/01/2024
HASH: 80426275 0d50b783588a001075b10fcc

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 1 de 23

Índice

1. ANTECEDENTES.....
2. OBJETO.....
3. MARCO LEGAL.....
4. ÁMBITO DE APLICACIÓN.....
5. VIGENCIA.....
6. REVISIÓN Y EVALUACIÓN.....
7. GENERAL.....
8. UTILIZACIÓN DEL EQUIPAMENTO INFORMÁTICO Y DE DISPOSITIVOS
8.1. ASIGNACIÓN, CONFIGURACIÓN Y USO SEGURO DE EQUIPOS Y DISPOSITIVOS.....
8.2. ALMACENAMIENTO SEGURO DE INFORMACIÓN
8.3. USO SEGURO DE EQUIPOS PORTÁTILES Y MÓVILES
8.4. USO SEGURO DE MEMORIAS USB.....
8.5. GRABACIÓN SEGURA DE CD/DVDs.....
8.6. BORRADO Y ELIMINACIÓN SEGURA DE SOPORTES.....
8.7. USO SEGURO DE IMPRESORAS, FOTOCOPIADORAS Y FAXES.....
8.8. DIGITALIZACIÓN SEGURA DE DOCUMENTOS.....
8.9. USOS PROHIBIDOS.....
9. PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA.....
10. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL.....
11. IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.....
12. ACCESO SEGURO DE TERCEROS A LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS.....
13. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO.....
14. TRATAMIENTO SEGURO DE LA INFORMACIÓN.....
15. SALIDA DE INFORMACIÓN.....
16. USO SEGURO DEL CORREO ELECTRÓNICO.....
16.1. NORMAS GENERALES.....
16.2. USOS PROHIBIDOS.....
16.3. RECOMENDACIONES ADICIONALES.....
17. ACCESO SEGURO A INTERNET Y USO DE HERRAMIENTAS DE COLABORACIÓN.....
17.1. NORMAS GENERALES.....
17.2. USOS PROHIBIDOS.....
18. INCIDENCIAS DE SEGURIDAD.....
19. ACTUALIZACIÓN DE LA INFORMACIÓN MUNICIPAL
20. USO ABUSIVO.....
20.1. USO ABUSIVO DEL ACCESO A INTERNET.....
20.2. USO ABUSIVO DEL CORREO ELECTRÓNICO.....
20.3. USO ABUSIVO DE OTROS SERVICIOS Y SISTEMAS DEL AYUNTAMIENTO
21. SUPERVISIÓN Y APLICACIÓN DE LA PRESENTE NORMATIVA.....
22. INCUMPLIMIENTO DE LA NORMATIVA.....
23. ANEXO: MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO.....

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 2 de 23

1. ANTECEDENTES.

Con fecha 26 de diciembre de 2012 fue aprobada la Ordenanza Reguladora del Uso de Medios Electrónicos del Ayuntamiento de Osuna (Boletín Oficial de la Provincia de Sevilla número 107 de 11 de mayo de 2013) donde se establece el marco general de actuación pala la implementación de la Administración Electrónica, y donde se establece la necesidad de elaborar su política de seguridad, identificando a los responsables encargados de velar por su cumplimiento, y ello de acuerdo a los principios básicos y requisitos mínimos establecidos en el Esquema Nacional de Seguridad.

Por Decreto de la Alcaldía número 2021-0482, de 29 abril de 2021 se crea y asignaron funciones al Comité de Seguridad de la Información del Ayuntamiento de Osuna, teniendo en cuenta la nueva realidad administrativa que gira en torno a las tecnologías de la información como soporte de servicios, con un impulso que se materializa con la aprobación de la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, donde se da un impulso definitivo a la implantación de los procesos electrónicos en las administraciones públicas, citando expresamente la necesidad de respetar un marco común de seguridad de la información. Además, con la entrada en vigor de ambas leyes se consagra la comunicación electrónica entre la Administración y la ciudadanía, haciéndose imprescindible garantizar el cumplimiento de los principios básicos y requisitos mínimos estableciendo las medidas de seguridad necesarias que habrán de ser proporcionales a las dimensiones de seguridad relevantes y a la categoría del sistema de información a proteger.

La presente Norma de Uso del sistema de Información del Ayuntamiento de Osuna deberá ser complementada, en su caso, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Así mismo resulta necesario hacer referencia al imperativo legal que impulsa la redacción de esta normativa, y es lo dispuesto en el art. 87.3 de la Ley Orgánica de Protección de Datos, 3/2018 de 5 de diciembre:

“Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.”

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 3 de 23

2. OBJETO.

De conformidad con lo dispuesto por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el presente documento tiene por objeto establecer la normativa para el buen uso del sistema de Información del Ayuntamiento de Osuna, señalando los compromisos que adquieren sus usuarios en relación con el cumplimiento normativo y el uso seguro de la información.

3. MARCO LEGAL.

Ordenanza Reguladora del Uso de Medios Electrónicos del Ayuntamiento de Osuna (Boletín Oficial de la Provincia de Sevilla número 107 de 11 de mayo de 2013)

Decreto de la Alcaldía número 2021-0482, de 29 abril de 2021 se crea y asignan funciones al Comité de Seguridad de la Información del Ayuntamiento de Osuna.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Ley Orgánica de Protección de Datos, 3/2018 de 5 de diciembre.

UNE - ISO/IEC 27001:2022 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.

UNE - ISO/IEC 27002:2022 Código de buenas prácticas para la Gestión de la Seguridad de la información.

4. ÁMBITO DE APLICACIÓN.

La presente normativa será de aplicación al ámbito de la Administración electrónica del Ayuntamiento y sus contenidos traen causa de las directrices definidas en su Política de Seguridad de la Información.

La presente normativa es de aplicación y de obligado cumplimiento para toda persona que, de manera permanente o eventual, preste sus servicios en el Ayuntamiento, incluyendo el personal de proveedores externos, cuando sean usuarios de su sistema de Información.

Se entiende por usuario, en el ámbito de la presente normativa, cualquier persona perteneciente a la plantilla del Ayuntamiento, así como personal de organizaciones privadas externas, entidades colaboradoras con algún tipo de vinculación con el Ayuntamiento que utilice o posea acceso a su sistema de Información.

La presente normativa establece obligaciones para el uso adecuado de los recursos de tratamiento de información que el Ayuntamiento de Osuna pone a disposición de sus

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 4 de 23

usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

5. REVISIÓN Y EVALUACIÓN.

La gestión de esta normativa corresponde al Comité de Seguridad de la información del Ayuntamiento , que es competente para:

Interpretar las dudas que puedan surgir en su aplicación.

Proponer su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la Responsable de Seguridad revisará la presente Normativa General, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad del Ayuntamiento.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

La Responsable de Seguridad del Ayuntamiento es la encargada de la custodia y divulgación de la versión aprobada de este documento. Todo ello sin perjuicio de la publicidad activa a la que dicho documento por su naturaleza jurídica deba estar sometido.

6. GENERAL.

El sistema de Información del Ayuntamiento integra todos los activos necesarios para el desarrollo de las competencias que tiene encomendadas la entidad, por lo que los usuarios utilizarán los recursos y servicios puestos a su disposición de manera que se garantice, en todo momento, la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de los servicios.

El uso de los equipos informáticos, dispositivos y redes de comunicaciones del Ayuntamiento por los usuarios tiene la finalidad de facilitar y agilizar la tramitación de procedimientos administrativos, mediante las aplicaciones de gestión, así como de poner a disposición de sus beneficiarios (ciudadanía, empresas, autónomos, etc.) una información completa, puntual, homogénea, actualizada y fiable.

Los equipos informáticos, dispositivos y redes de comunicaciones del Ayuntamiento se ponen a disposición de los usuarios como herramientas de trabajo para el desempeño de su actividad laboral, razón por la cual compete a la Responsable de Seguridad del Ayuntamiento determinar las condiciones de seguridad y responsabilidades bajo las cuales se deben utilizar tales recursos.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 5 de 23

En consecuencia, la presente normativa tiene como objetivo establecer las pautas de obligado cumplimiento para garantizar la seguridad y privacidad de la información y la disponibilidad de los servicios de Administración electrónica prestados por el Ayuntamiento.

7. UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE DISPOSITIVOS.

El Ayuntamiento facilita los equipos informáticos y dispositivos, tanto fijos como móviles, necesarios para el desempeño de la actividad laboral de los usuarios.

Los equipos, dispositivos, aplicaciones, redes de comunicaciones, datos y servicios de Administración electrónica que el Ayuntamiento pone a disposición de los usuarios deberán utilizarse exclusivamente para el desempeño de su actividad laboral. Cualquier otro uso con fines distintos a los autorizados está estrictamente prohibido.

El ordenador personal, incluyendo los equipos de sobremesa, portátiles y dispositivos móviles, será el equipamiento informático que permitirá el acceso seguro de los usuarios al sistema de Información del Ayuntamiento, constituyendo el componente más crítico de la seguridad de información, razón por la que estará debidamente configurado por el Servicio de Informática y su adecuada utilización está regulado por las políticas y la normativa interna del Ayuntamiento.

8. ASIGNACIÓN, CONFIGURACIÓN Y USO SEGURO DE EQUIPOS Y DISPOSITIVOS.

Los equipos informáticos serán asignados por el Servicio de Informática del Ayuntamiento a cada usuario debidamente configurados y con acceso a los servicios y aplicaciones necesarias para su desempeño laboral.

Cada equipo informático y/o dispositivo de comunicación estará asignado a un único usuario nominal, responsable de su uso, salvo aquellos instalados para el acceso público a Internet.

Únicamente el personal autorizado por el Servicio de Informática del Ayuntamiento podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan comprometer la seguridad del sistema de Información del Ayuntamiento.

El Responsable del Servicio de Informática del Ayuntamiento deberá autorizar, con anterioridad a su uso laboral, cualquier equipamiento informático o dispositivo no proveído por el Ayuntamiento.

Está prohibido alterar, sin la debida autorización del Responsable del Servicio de Informática del Ayuntamiento, cualquiera de los componentes físicos o lógicos de los equipos

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 6 de 23

informáticos y dispositivos. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

Los usuarios no tendrán privilegio de administración sobre los equipos informáticos y dispositivos, salvo autorización expresa del Responsable del Servicio de Informática del Ayuntamiento.

Los usuarios están obligados a facilitar al personal del Servicio de Informática del Ayuntamiento el acceso a sus equipos para labores de respuesta a incidentes, instalación o mantenimiento. Este acceso se limitará únicamente a las intervenciones necesarias que pudieran encontrarse en el uso del equipamiento informático y de comunicaciones.

Si el personal del Servicio de Informática del Ayuntamiento detectase cualquier anomalía que indicará una utilización de los equipos informáticos y dispositivos de comunicación contraria a la presente norma, lo pondrá en conocimiento de la Responsable de Seguridad, que tomará las oportunas medidas correctoras en el ámbito de sus competencias, dando traslado de la incidencia al Responsable de Recursos Humanos del Ayuntamiento.

Los equipos informáticos y dispositivos de comunicación de los usuarios deberán mantener al día las actualizaciones de seguridad, obligándose estos a facilitar su debida instalación. Se prestará especial atención a la correcta actualización, configuración y funcionamiento de las aplicaciones de seguridad antivirus, antispam, cortafuegos, etc.

Los usuarios deberán notificar al Responsable del Servicio de Informática del Ayuntamiento a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

El usuario deberá ser consciente que las amenazas de ciberseguridad, tales como virus, troyanos, etc. requieren de su participación de para propagarse, ya sea a través de memorias USB, mensajes de correo electrónico, etc. o mediante la descarga e instalación de programas desde Internet.

El usuario será responsable de toda la información extraída fuera del Ayuntamiento, a través de dispositivos tales como memorias USB. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información de uso oficial o confidencial y someterse a los protocolos de autorización establecidos.

El cese de actividad de cualquier usuario deberá ser comunicado por su Responsable del área municipal a la que estuviera asignado de forma inmediata a al Responsable del Servicio de Informática del Ayuntamiento al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 7 de 23

Correlativamente, el usuario tendrá la obligación de la devolución inmediata al personal del Servicio de Informática del Ayuntamiento cuando finalice su vinculación con el Ayuntamiento.

9. ALMACENAMIENTO SEGURO DE INFORMACIÓN.

El Ayuntamiento pondrá a disposición de los usuarios de unidades de red compartidas para la realización de copias de seguridad de sus unidades locales.

Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios no será objeto de salvaguarda mediante copia de seguridad.

Cuando el almacenamiento local esté autorizado por el Responsable del Servicio de Informática del Ayuntamiento, los usuarios deberán realizar copias semanales de seguridad de la información generada en su actividad profesional.

Las unidades de almacenamiento de datos del Ayuntamiento son un recurso limitado y compartido por todos los usuarios, por lo que el Servicio de Informática realizará las copias de seguridad para salvaguardar la continuidad de los servicios de la Administración electrónica.

Los datos generados por el usuario en el desempeño de sus competencias laborales deberán mantenerse en una unidad de red compartida.

Los usuarios autorizados a almacenar información en forma local (por ejemplo, en el disco duro del equipo asignado) serán responsables de realizar sus copias de seguridad. En general, se desaconseja que los usuarios almacenen sus ficheros de trabajo fuera de las carpetas de red habilitadas al efecto.
De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red compartidas del Ayuntamiento. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en los equipos de usuario.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al Servicio de Informática del Ayuntamiento.

10. USO SEGURO DE EQUIPOS PORTÁTILES Y MÓVILES.

Los equipos portátiles y dispositivos móviles, incluyendo los teléfonos móviles y las tabletas, serán asignados a los usuarios por Servicio de Informática del Ayuntamiento.

Estos dispositivos quedarán bajo la custodia del usuario al que se le asigne, debiendo adoptar las medidas de protección indicadas por las políticas y la normativa del Ayuntamiento para evitar daños, extravío o sustracción, así como el acceso no autorizado a la información que almacenan.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 8 de 23

La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Responsable del Servicio de Informática del Ayuntamiento para la adopción de las medidas que correspondan.

Los equipos portátiles y dispositivos móviles deberán utilizarse únicamente para fines laborales y autorizados, especialmente cuando se usen fuera de las dependencias e instalaciones municipales, salvo autorización expresa.

Los usuarios de equipos portátiles y dispositivos móviles se responsabilizarán de que no serán usados por terceras personas o entidades no autorizadas por el Responsable del Servicio de Informática del Ayuntamiento.

Los equipos portátiles no deberán conectarse directamente a redes de comunicaciones externas, incluyendo la red o el acceso a Internet del usuario en su domicilio, excepto cuando haya sido autorizados por el Responsable del Servicio de Informática del Ayuntamiento.

El Ayuntamiento podrá proporcionar accesos remotos autorizados y configurados por Servicio de Informática del Ayuntamiento a través de conexiones VPN. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos. En casos debidamente justificados y previamente autorizados por Servicio de Informática del Ayuntamiento se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente normativa que resulten de aplicación.

Los usuarios de equipos portátiles y dispositivos móviles deberán realizar conexiones, al menos, mensuales a la red corporativa municipal de comunicaciones, siguiendo las instrucciones proporcionadas por Servicio de Informática del Ayuntamiento, para permitir la actualización de las aplicaciones informáticas, el sistema operativo, el antivirus y demás aplicaciones de seguridad. En su defecto, cada trimestre los equipos portátiles y dispositivos móviles deberán ser puesto a disposición del Servicio de Informática para su actualización.

Los equipos portátiles y dispositivos móviles deberán tener el disco duro o unidad de almacenamiento cifrado, de aplicaciones de seguridad activadas que garanticen una configuración segura, así como de un registro de actividad de los usuarios.

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, Bluetooh, USB, HDMI, DVD, etc.). No obstante, se podrán habilitar algunas o todas las funciones de salida de información mediante autorización del Responsable de Servicio de Informática del Ayuntamiento.

Está prohibido alterar, sin la debida autorización del Responsable del Servicio de Informática del Ayuntamiento, cualquiera de los componentes físicos o lógicos de los equipos portátiles

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 9 de 23

y dispositivos móviles. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

Los usuarios no tendrán privilegio de administración sobre los equipos portátiles y dispositivos móviles, salvo autorización expresa del Responsable del Servicio de Informática del Ayuntamiento.

Cuando se modifiquen las circunstancias profesionales (baja laboral, término de una tarea, cese en el cargo, etc.) que originaron la asignación de equipos portátiles y dispositivos móviles, el usuario lo devolverá al Servicio de Informática del Ayuntamiento al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original.

11. USO SEGURO DE MEMORIAS USB.

Con carácter general, el uso de memorias USB en el Ayuntamiento no está autorizado. En su caso, la autorización deberá proporcionarla Responsable del Servicio de Informática del Ayuntamiento.

Los puertos USB de los equipos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, requerirá la autorización del Responsable del Servicio de Informática del Ayuntamiento.

En el caso de que a un usuario se le autorice el uso de puertos USB de su equipo personal, las memorias USB utilizadas serán las proporcionadas por el Ayuntamiento, que serán conformes a las normas de seguridad. Las memorias USB proveídas por el Ayuntamiento serán de uso exclusivo en los equipos de usuario, no debiendo ser usados fuera de éstos.

Las memorias USB están destinadas a un uso exclusivamente laboral, como medio de transporte de ficheros, no como unidad de almacenamiento. Servicio de Informática del Ayuntamiento pondrá a disposición de los usuarios las unidades de almacenamiento en red para tal propósito.

La pérdida o sustracción de una memoria USB deberá ponerse en conocimiento, con indicación de su contenido y de forma inmediata, al Responsable del Servicio de Informática del Ayuntamiento.

12. GRABACIÓN SEGURA DE CD/DVDs.

Con carácter general, el uso de equipos grabadores de CD/DVDs en el Ayuntamiento no está autorizado. En su caso, la autorización deberá proporcionarla la Responsable del Servicio de Informática del Ayuntamiento.

Las unidades de grabación de CDs y DVDs de los puestos de trabajo de los usuarios estarán deshabilitados. En caso de ser necesaria su habilitación, requerirá la autorización del

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 10 de 23

Responsable del Servicio de Informática del Ayuntamiento.

13. BORRADO Y ELIMINACIÓN SEGURA DE SOPORTES.

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

Asegurarse del contenido de cualquier soporte antes de su eliminación.

Cuando contenga información de uso interno o confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por el Ayuntamiento.

Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente Responsable del Servicio de Informática del Ayuntamiento, que será responsable de la destrucción o almacenamiento de los medios informáticos obsoletos.

14. USO SEGURO DE IMPRESORAS, FOTOCOPIADORAS Y FAXES.

Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras de uso compartido del Ayuntamiento

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 Responsable del Servicio de Informática del Ayuntamiento.

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

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.

No olvidar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación abandonada, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente.

Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, para evitar que terceras personas puedan acceder al mismo. Si se encontrase documentación abandonada, 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 Servicio de Informática del Ayuntamiento.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 11 de 23

15. DIGITALIZACIÓN SEGURA DE DOCUMENTOS.

Con carácter general, cuando se digitalicen documentos el usuario deberá prestar especial cuidado con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información confidencial.

No olvidar recuperar los originales del escáner, una vez finalizada la digitalización. Si se encontrase documentación abandonada, 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 Servicio de Informática del Ayuntamiento.

16. USOS PROHIBIDOS.

Están terminantemente prohibidos los siguientes comportamientos:

La descarga, instalación y utilización de aplicaciones informáticas no proveídas por el Ayuntamiento, sin la previa autorización del Responsable del Servicio de Informática del Ayuntamiento.

La conexión a la red informática de cualquier equipo o dispositivo no proveído por el Ayuntamiento, sin la previa autorización del Responsable del Servicio de Informática del Ayuntamiento

La utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por la Responsable del Servicio de Informática del Ayuntamiento.

La utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa Responsable del Servicio de Informática del Ayuntamiento.

El almacenamiento de información privada , de cualquier naturaleza, por los usuarios del Ayuntamiento en los medios de almacenamiento compartidos o locales.

La alteración de cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación. En los casos autorizados, las operaciones de modificación sólo podrán realizarse por el personal de soporte técnico del Servicio de Informática del Ayuntamiento.

La ejecución remota de archivos de tipo audiovisual (música, vídeo, etc.).

La descarga, Instalación y/o utilización de aplicaciones informáticas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual.

La suplantación de identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 12 de 23

La destrucción o modificación no autorizada de la información del Ayuntamiento, de manera premeditada.

La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

El deterioro intencionado del trabajo de otras personas del Ayuntamiento.

El uso de los sistemas de información para fines ajenos a los del Ayuntamiento.

Dañar intencionadamente los recursos informáticos del Ayuntamiento o de otras instituciones.

Incurrir en cualquier otra actividad ilícita, del tipo que sea.

Estos comportamientos estarán sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

17. PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA.

La documentación impresa que contenga datos confidenciales debe ser especialmente protegida, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

Cuando concluya la vida útil de los documentos impresos con información confidencial, deberán ser eliminados en las máquinas destructoras del Ayuntamiento, de forma que no sea recuperable la información que pudieran contener o en su defecto por empresa contratada a tal fin.

Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información confidencial.

Por razones de sostenibilidad y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

18. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL.

Está estrictamente prohibida la ejecución de aplicaciones informáticas sin la correspondiente licencia de uso.

Las aplicaciones informáticas licenciadas o propiedad del Ayuntamiento están protegidos por

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 13 de 23

la legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa de la Responsable de Seguridad del Ayuntamiento.

Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra del Ayuntamiento protegida por derechos de Propiedad Intelectual.

19. IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.

Todos los usuarios dispondrán de un nombre de usuario y una contraseña o bien una tarjeta criptográfica con certificado digital, para el acceso al sistema de Información del Ayuntamiento, siendo responsables de su custodia y de toda actividad relacionada con el uso de su acceso autorizado.

El nombre de usuario será único para cada usuario del Ayuntamiento, intransferible e independiente del puesto de trabajo desde el que se realiza el acceso al sistema de información.

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

Los usuarios no utilizaran, en ningún caso, el acceso de otro usuario.

Si un usuario tiene sospechas de que sus credenciales de acceso están siendo utilizadas por otra persona, lo comunicará inmediatamente al Servicio de Informática.

Si un usuario recibiera una llamada telefónica, SMS o cualquier otro tipo de comunicación solicitando su nombre de usuario y contraseña, nunca facilitará dichos datos y lo comunicará inmediatamente al Servicio de Informática del Ayuntamiento.

20. ACCESO SEGURO DE TERCEROS A LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS.

Los terceros o personas ajenas al Ayuntamiento que accedan a los edificios, instalaciones o dependencias del Ayuntamiento, seguirán las siguientes normas:

Para acceder a los edificios, instalaciones o dependencias del Ayuntamiento se deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI, NIE, pasaporte, etc.), registrándose por el personal de Control de Acceso, que solicitará la presencia de la persona responsable del Ayuntamiento, que supervisará su estancia o visita.

La acreditación personal que se le proporcione en el Control de Acceso deberá portarse en lugar visible en todo momento, debiendo ser entregada a la salida.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 14 de 23

Una vez en el interior de los edificios, dependencias o instalaciones del Ayuntamiento, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo o zona a que les haya sido autorizado y en las zonas de uso común (aseos, cafetería, etc.).

Asimismo, deberán tener autorización cuando tengan necesidad de realizar desplazamientos entre distintas dependencias del Ayuntamiento.

Los terceros atendrán siempre los requerimientos que le hiciere el personal de control y seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

Cualquier incidencia que surja antes o en el transcurso de la estancia de terceros al Ayuntamiento, deberán ponerla en conocimiento de su responsable, que dará asesoramiento, atender consultas o necesidades, transmitir instrucciones, ponerle al corriente de sus cometidos, objetivos, etc.

21. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO.

Los datos de carácter personal tratados por el Ayuntamiento están protegidos por la normativa vigente, europea y nacional.

Todo usuario del Ayuntamiento o de terceras organizaciones que, en virtud de su actividad laboral, pudiera tener acceso o tratar datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con el Ayuntamiento, así como a observar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

22. TRATAMIENTO SEGURO DE LA INFORMACIÓN.

Toda la información contenida en el sistema de información del Ayuntamiento o que sea transmitida por sus redes de comunicaciones deberá ser utilizada únicamente para el cumplimiento de las funciones encomendadas al Ayuntamiento y a su personal.

Queda prohibido transmitir o alojar información confidencial o datos de carácter personal del Ayuntamiento en servidores externos salvo autorización expresa de la Responsable de Seguridad, que comprobará la inexistencia de trabas legales y verificará la suscripción de un contrato expreso entre el Ayuntamiento y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, Acuerdo de encargo de tratamiento de datos personales, en su caso, así como el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

Los terceros o personas ajenas al Ayuntamiento que temporalmente deban acceder al sistema de información deberán hacerlo siempre bajo la supervisión de algún responsable del Ayuntamiento y previa autorización de la Responsable de Seguridad.

Para los accesos de terceros a los sistemas de información del Ayuntamiento se habilitarán usuarios temporales que serán eliminados una vez concluido su trabajo.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 15 de 23

Los terceros o personas ajenas al Ayuntamiento, en lo que les sea de aplicación, deberán cumplir puntualmente la presente normativa, así como el resto de normativa de seguridad del Ayuntamiento, especialmente en lo referente a los apartados de salida y confidencialidad de la información.

23. SALIDA DE INFORMACIÓN.

La salida de información de los edificios, instalaciones o dependencias del Ayuntamiento, en cualquier soporte o por cualquier medio de comunicación, deberá ser realizada exclusivamente por personal autorizado por el Responsable del Servicios de Informática del Ayuntamiento, autorización que contemplará igualmente a la propia información que sale.

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

Los usuarios se abstendrán de sacar al exterior cualquier información del Ayuntamiento, independientemente del dispositivo de soporte (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

24. USO SEGURO DEL CORREO ELECTRÓNICO.

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios del Ayuntamiento para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo municipal.

Se trata de un recurso compartido del Ayuntamiento, por lo que un uso indebido afecta de manera directa a todos los usuarios remitentes y destinatarios.

NORMAS GENERALES.

Todo usuario del Ayuntamiento dispondrá de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos.

Los usuarios únicamente utilizarán la aplicación de correo electrónico suministrada, instalada y configurada por el Servicio de Informática del Ayuntamiento.

El correo electrónico del Ayuntamiento se utilizará, única y exclusivamente, para el desempeño laboral de los usuarios, quedando totalmente prohibido el uso privado del mismo.

Se deberá notificar puntualmente al Servicio de Informática del Ayuntamiento cualquier anomalía o incidencia observada, así como la recepción de correos no deseados (“spam”) a fin de tomar las medidas de seguridad oportunas.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 16 de 23

Se prestará especial atención a los ficheros adjuntos en los correos recibidos, que no deberán abrirse ni ejecutarse, cuando se e sospeche que los ficheros provengan de fuentes desconocidas o no fiables, puesto que podrían contener virus o código malicioso. En estos casos, se deberá notificar puntualmente al Servicio de Informática del Ayuntamiento a fin de tomar las medidas de seguridad oportunas.

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

USOS PROHIBIDOS.

Las siguientes actuaciones están explícitamente prohibidas:

El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad.

El envío de correos electrónicos 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 al propio sistema de información del Ayuntamiento.

El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.

La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad laboral del usuario.

Responder mensajes de los que se tenga sospechas sobre su autenticidad y contenido o mensajes que contengan publicidad no deseada.

El uso del correo electrónico para intercambio de ficheros adjuntos de tamaño superior a 3 Mb.

El uso del correo electrónico para el envío de información sensible, confidencial o protegida.

El uso del correo electrónico para recoger correo de buzones que no pertenezcan al Ayuntamiento o el reenvío automático del correo corporativo a buzones ajenos al Ayuntamiento.

RECOMENDACIONES ADICIONALES.

Asegurarse que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

Evitar el uso ineficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 17 de 23

en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.

Evitar el uso de los buzones de correo para el almacenamiento de información.

Evitar el envío de correos fuera del horario laboral a efectos de desconexión digital.

25. ACCESO SEGURO A INTERNET Y USO DE HERRAMIENTAS DE COLABORACIÓN.

El servicio de acceso a Internet es un recurso que el Ayuntamiento pone a disposición de los usuarios, como herramienta necesaria para el desempeño de su actividad laboral.

El Ayuntamiento velará por el buen uso del acceso a Internet, desde el punto de vista de la eficiencia y productividad, como de la seguridad de su uso.

NORMAS GENERALES

El acceso a Internet estará autorizado por el Responsable del Servicio de Informática del Ayuntamiento para el desempeño de la actividad laboral del usuario.

Las conexiones que se realicen a Internet deberán obedecer a fines laborales.

El acceso a Internet con fines personales se autoriza únicamente en casos excepcionales, siempre que no interfiera en el desempeño laboral.

Sólo se autoriza el acceso a Internet a través de la aplicación de navegador suministrado y configurado por el Servicio de Informática del Ayuntamiento.

No podrá alterarse la configuración segura de la aplicación de navegador suministrado y configurado por el Servicio de Informática del Ayuntamiento ni utilizar un navegador alternativo.

Deberá notificarse puntualmente al Servicio de Informática del Ayuntamiento cualquier anomalía o incidencia detectada en el uso de Internet, para la determinación de las medidas de seguridad oportunas.

USOS PROHIBIDOS

Quedan prohibidas las siguientes actuaciones:

La descarga de archivos voluminosos.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 18 de 23

La descarga de programas informáticos sin la autorización previa del Responsable del Servicio de Informática del Ayuntamiento o de ficheros con potencial contenido dañino.

Asegurarse que los sitios web visitados sean de confianza.

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

La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.).

INCIDENCIAS DE SEGURIDAD.

Cualquier usuario que detecte o sospeche de una potencial anomalía o incidencia de seguridad deberá informar inmediatamente al Servicio de Informática del Ayuntamiento, para la determinación de las medidas de seguridad oportunas.

ACTUALIZACIÓN DE LA INFORMACIÓN MUNICIPAL.

Las modificación de la información contenida en las bases de datos municipales deberá realizarse por usuarios autorizados y estará siempre relacionada por un expediente administrativo que justifique los cambios o la carga de ficheros de información suministrados y debidamente registrados en los registros de entrada/salida, de acuerdo con los procedimientos administrativos establecidos.

Se prohíbe realizar cualquier actualización en las bases de datos de información municipal desde cualquier aplicación no proveída o autorizada por el Ayuntamiento.

El Ayuntamiento podrá habilitar la monitorización del acceso y/o la modificación de la información, que quedarán registrados para su auditoría.

USO ABUSIVO.

El uso de Internet, del correo electrónico y el acceso al resto de los servicios de Administración electrónica del Ayuntamiento estará monitorizado por el Servicio de Informática del Ayuntamiento.

Si se hiciese un uso abusivo o inapropiado de estos recursos o servicios, el Ayuntamiento podrá adoptar las medidas disciplinarias oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

USO ABUSIVO DEL ACCESO A INTERNET.

Acceder a contenidos no relacionados con los cometidos laborales del usuario.

Acceder a otras redes, con el propósito de violar su integridad o seguridad.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 19 de 23

Acceder, recuperar o visualizar textos o gráficos que excedan los límites de la ética.

Almacenar en la estación de trabajo del usuario o en los servidores del Ayuntamiento archivos personales.

Utilizar el acceso a Internet para el uso de mensajería instantánea (Messenger, Skype, etc.).

Transferir contenidos no relacionados con el desempeño laboral del usuario (juegos, ficheros de sonido, fotos, videos o películas, etc.).

Realizar cualquier actividad de promoción de intereses personales.

Publicar o enviar información no solicitada.
Publicar o enviar información sensible, confidencial, protegida o propiedad del Ayuntamiento, a personas, empresas o sistemas de información externos no autorizados. En este sentido, los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.

Publicar o enviar mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo cualquier norma interna que pudiera resultar de aplicación.

Emplear utilidades de intercambio de información en Internet (tales como redes P2P).

Usar Internet para propósitos que puedan influir negativamente en la imagen del Ayuntamiento, de sus representantes o de los organismos públicos o privados con los que se mantiene relación institicional.

USO ABUSIVO DEL CORREO ELECTRÓNICO.

Utilizar el correo electrónico para fines distintos al desempeño laboral del usuario, más en concreto, los que siguen:

Intercambiar contenidos (textos o gráficos) que excedan los límites de la ética.

Transferir ficheros ajenos al desempeño laboral del usuario (software sin licencia, ficheros de sonido, fotos y videos, gráficos, virus, código malicioso, etc.).

Realizar cualquier actividad de promoción de intereses personales.

Usar una cuenta de correo electrónico del Ayuntamiento de Osuna para enviar mensajes o cartas en cadena y/o correos basura o *spam* (correo electrónico no solicitado).

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

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 20 de 23

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

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

USO ABUSIVO DE OTROS SERVICIOS Y SISTEMAS DEL AYUNTAMIENTO

Acceder a servicios y/o contenidos del Ayuntamiento con el propósito de violar su integridad o seguridad.

Acceder, recuperar, o visualizar textos o gráficos que excedan los límites de la ética.
Almacenar archivos personales en la estación de trabajo o en los servidores del Ayuntamiento.

Usar mensajería instantánea (Messenger, Skype, etc.) no autorizada.

Transferir ficheros entre usuarios del Ayuntamiento no relacionados con las actividades laborales.

Realizar cualquier actividad de promoción de intereses personales.
El uso de cualquier servicio del Ayuntamiento para:

La publicación o envío de información no solicitada.

La publicación o envío de información confidencial, propiedad del Ayuntamiento, a personas, empresas o sistemas de información externos no autorizados. Los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.

El uso de los servicios del Ayuntamiento para propósitos que puedan influir negativamente en la imagen del Ayuntamiento, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

El envío de mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.

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

El Ayuntamiento implantará los sistemas de protección de acceso al sistema de información necesarios para evitar incidentes o incumplimientos relacionados con el abuso de estos

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 21 de 23

servicios.

SUPERVISIÓN Y APLICACIÓN DE LA PRESENTE NORMATIVA.

El Ayuntamiento, por motivos legales, de seguridad y/o de calidad del servicio, y cumpliendo, en todo momento, los requisitos que establece la legislación vigente, podrá:

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

Monitorizar los accesos a la información contenida en su sistema de información.

Auditar la seguridad de las credenciales y aplicaciones.

Monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.

El Ayuntamiento llevará a cabo la monitorización de manera proporcionada, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios.

El servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún incidente de seguridad o incumplimiento de la presente Normativa.

El Ayuntamiento podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.

Igualmente, se podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados.

INCUMPLIMIENTO DE LA NORMATIVA

Todo usuario del Ayuntamiento está obligado a cumplir lo prescrito en la presente Normativa de Uso Seguro de la información y los servicios de Administración electrónica.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa de Uso Seguro de la información y los servicios de Administración electrónica, serán exigidas las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales.

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 22 de 23

ANEXO: MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, como usuario del sistema de información del Ayuntamiento de Osuna, declara haber leído y comprendido la "Normativa de Uso Seguro de la información y los servicios de Administración electrónica del Ayuntamiento de Osuna" (V1.0) y se compromete, bajo su responsabilidad, a su debido cumplimiento.

<<A FECHA DE FIRMA ELECTRÓNICA.>>

Cód. Validación: 93R3TQJDEXH5SLZ22RMWJL5YD
Verificación: https://osuna.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 23 de 23