



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

REGLAMENTO DEL USO DE LOS RECURSOS Y ACCESOS A LOS SISTEMAS DE INFORMACIÓN DEL AYUNTAMIENTO DE HUESCA.

CAPÍTULO I. OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1. Objeto

El tratamiento de la información y, en particular, de los datos personales, mediante el uso de sistemas de información es esencial en la operativa diaria del Ayuntamiento de Huesca, y se lleva a cabo en el desempeño habitual de las tareas de muchos de sus empleados. El tratamiento de esta información de manera incorrecta supondrá una serie de riesgos que podrán menoscabar la privacidad y derechos de los interesados y los intereses del Ayuntamiento de Huesca. La prevención efectiva frente a estos riesgos es una tarea clave de todo el personal municipal.

El propósito de este documento es, por lo tanto, describir el uso aceptable de los recursos o/y sistemas de información que englobamos en Plataformas de la Tecnología de la Información del Ayuntamiento de Huesca (en adelante, Plataformas TI). Así, este documento tiene por objeto:

- a) Proteger la información del Ayuntamiento de Huesca o bajo su responsabilidad, que se procesa y/o accede a través de las Plataformas TI.
- b) Garantizar el correcto funcionamiento y la gestión eficiente de las Plataformas TI.
- c) Garantizar el cumplimiento de todas las leyes y reglamentos aplicables relacionados con los derechos de propiedad intelectual e industrial y la protección de datos personales, entre otros.

Las Plataformas TI son todo el material o servicio tecnológico que el Ayuntamiento de Huesca ha puesto a disposición de los usuarios para desarrollar su labor. Entre ellos, pero sin limitación, se encuentran los Sistemas TI, los Equipos de Redes y Comunicaciones, el Cableado TI, el Parque de Puesto de Trabajo Digital (PC, portátil, Tablet, smartphones, ...), los Soportes TI (Discos y memorias externas), los Dispositivos Conectados etc.

Artículo 2. Ámbito de aplicación

1. Mediante la presente normativa, el Ayuntamiento de Huesca regula el uso de los recursos tecnológicos de su sistema de información a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal del Ayuntamiento, tanto laboral como funcionario, así como aquellas personas que mantienen otra relación con la entidad local (cargos políticos, personal de confianza, becarios, personal en prácticas, etc.), los cuales quedan sujetos a la misma, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

Plaza de la Catedral 1, 22002 Huesca CIF P2217300I
Registro de las Entidades Locales Número 01221259 Teléfono (974) 29 21 00 Fax (974) 29 21 63
www.huesca.es



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

2. Lo expuesto en el primer apartado del presente artículo será de aplicación igualmente a aquellos entes dependientes del Ayuntamiento de Huesca, así como al conjunto del sector público institucional local (organismos Autónomos, sociedades municipales, etc.).

3. También será de aplicación al personal de terceros con acceso al sistema (empresas proveedoras o colaboraciones reguladas por convenios), quienes quedan también sujetos a la misma, en la medida que le sean de aplicación, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el desempeño de sus actividades en el Ayuntamiento.

Artículo 3. Órganos y personas físicas responsables

1. El Comité de Seguridad de la Información será el órgano colegiado que se constituye como el máximo órgano decisorio en materia de seguridad de la información y protección de datos de carácter personal del Ayuntamiento de Huesca, y por lo tanto, es el órgano responsable de proporcionar las directrices de gestión de la seguridad de la información.

2. El Responsable del Sistema será la persona encargada de revisar y aprobar solicitudes de acceso a la información que estén dentro del Sistema; respetando siempre las leyes y reglamentos aplicables.

3. Corresponderá al Servicio de Nuevas Tecnologías:

a) Establecer medidas preventivas de monitorización e investigar posibles incidencias TI, que incluyen las ciberincidencias, manteniendo siempre segura y confidencial cualquier información a la que se acceda durante el proceso.

b) Notificar al Delegado de Protección de Datos las posibles brechas de seguridad en el tratamiento de de datos personales o durante la investigación de una ciberincidencia.

c) Asesorar y gestionar autorizaciones a excepciones a esta normativa.

d) Evaluar y autorizar la contratación y el uso de servicios y Plataformas TI en el Ayuntamiento de Huesca.

e) Auditar o probar la seguridad de las Plataformas TI, manteniendo siempre seguros y secretos la información confidencial y los datos personales a los que se accede.

f) Desarrollar procedimientos, protocolos e instrucciones para implementar esta normativa.

4. La Oficina de Seguridad y Protección de Datos será responsable del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información.

5. Los jefes de los distintos servicios municipales serán responsables de:



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

- a) Apoyar y facilitar a los usuarios bajo su responsabilidad, el cumplimiento de los requisitos establecidos en esta normativa, y en el resto de las instrucciones, protocolos, manuales y notas de concienciación que la desarrollen.
- b) Realizar solicitudes de acceso necesarias a Plataformas TI, mantener la segregación necesaria de tareas entre los usuarios y revisar y solicitar periódicamente la retirada de autorizaciones de acceso TI cuando ya no sean necesarios para los usuarios.

CAPÍTULO II. NORMATIVA DE USO DE RECURSOS Y ACCESO A SISTEMAS DE INFORMACIÓN

Artículo 4. Normas generales

1. El Ayuntamiento de Huesca pondrá a disposición de los usuarios las Plataformas TI necesarias para el desarrollo de sus funciones. Esto incluye puestos de trabajo (PC, portátil, pantalla, teléfono IP, smartphones, ...), aplicaciones y programas informáticos, cuentas de usuario y credenciales, correo electrónico, acceso a internet, accesos a carpetas de información en servidores o en la nube, etc.
2. Las plataformas TI y todos los archivos, mensajes, información o datos personales almacenados o transmitidos a través de dichos recursos informáticos son propiedad del Ayuntamiento de Huesca.
3. Las Plataformas TI del Ayuntamiento de Huesca serán para fines que sólo sirven a los intereses del Ayuntamiento y no podrán ser utilizados para el beneficio propio de los usuarios o terceras personas. En particular, no se permitirá el almacenamiento de datos no relacionados con el desempeño de las funciones propias del puesto de trabajo en las plataformas TI municipales.
4. Estará expresamente prohibido el uso de las Plataformas TI del Ayuntamiento de Huesca para cualquier actividad que sea ilegal bajo las leyes y regulaciones locales, nacionales o internacionales, o para llevar a cabo acciones que menoscaben los derechos de otros usuarios, y entre otras, las siguientes:
 - a) Participar en actividades a través de Plataformas TI que pueden acosar, amenazar o abusar de otras personas. Acceder, crear, almacenar o transmitir material ofensivo, indecente, obsceno o calumnioso.
 - b) Grabar cualquier voz, vídeo o reunión utilizando Plataformas TI sin autorización previa del responsable.
 - c) Acceder o intentar obtener acceso a las Plataformas TI de otros usuarios sin el conocimiento y el consentimiento de dicha persona, salvo en los casos debidamente autorizados.
5. Los departamentos o servicios municipales deberán comunicar al Servicio de Nuevas Tecnologías, con tiempo suficiente, las altas y bajas de los



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

usuarios en ese departamento o servicios y las plataformas TI y credenciales de acceso que van a necesitar o van a dejar de usar para proceder a su configuración.

6. En la fecha de la terminación de la relación funcionarial, contractual o política entre el usuario y el Ayuntamiento de Huesca, todos los recursos informáticos e información confidencial, que están en posesión de los usuarios deberán ser devueltos al Servicio de Nuevas Tecnologías, incluyendo, cualquier PC, ordenador portátil, teléfonos, dispositivos externos, documentos, archivos (en cualquier formato) y manuales. La información devuelta deberá ser accesible (desbloqueada y descifrada), y cualquier copia o copia adicional en posesión de los usuarios deberá ser destruida, incluyendo correos electrónicos, chats y mensajes relacionados con el trabajo.

Artículo 5. Normas relativas a la información y formación a los usuarios sobre el uso de los recursos y accesos a los sistemas informáticos.

1. Todos los usuarios tendrán la obligación de colaborar con los responsables designados por la entidad para velar por el cumplimiento de la legislación vigente en materia de seguridad de la información y en protección de datos personales. En particular, cada usuario deberá conocer sus obligaciones en el tratamiento de datos personales y utilización de sistemas de información, recogidas en el presente reglamento.

2. Deberá informarse a cada usuario que trabaje con las diversas plataformas TI puestas a su disposición, de los deberes y responsabilidades en materia de seguridad de la información. Los usuarios recibirán la formación necesaria, técnica y jurídica, para realizar un uso adecuado de las Plataformas TI y, en particular, para el uso adecuado de la información y datos personales contenidos en ella.

3. Habrá comunicación y divulgación periódica de información de seguridad, de manera que desde el Servicio de Nuevas Tecnologías o a través del Delegado de Protección de Datos, se enviarán periódicamente, mediante correo electrónico o el canal habilitado para ello, consejos de buen uso de los sistemas, notas de concienciación y divulgación, manuales de uso e instrucciones para un uso adecuado de las Plataformas TI, que deberán ser tenidos en cuenta por todos los usuarios. Esta información también estará disponible en el Portal del Empleado y en la intranet municipal.

Artículo 6. Normas de acceso a la información a través de Plataformas TI

1. La información estará debidamente protegida y será accesible a los usuarios autorizados a través de las Plataformas TI municipales habilitadas para ello, y mediante el uso de las credenciales únicas asignadas a cada usuario. De esta manera, cualquier acceso a la información o cualquier actividad en los sistemas de información estará registrado e identificado de forma única. El usuario



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

es el único responsable de todas las acciones realizadas con sus credenciales asignadas para acceder y usar las Plataformas TI.

2. De forma predeterminada, las cuentas genéricas (o compartidas) no estarán autorizadas en el Ayuntamiento de Huesca. Las excepciones a esta regla podrán ser aprobadas por el Comité de Seguridad de la Información cuando la trazabilidad se mantenga de otras maneras, o dicha trazabilidad no sea específicamente necesaria para ese uso en esas Plataformas TI.

3. Las credenciales serán del tipo que indique las políticas, procedimientos y directrices del Ayuntamiento de Huesca (usuario/contraseña, certificados electrónicos u otros factores de autenticación), tendrán la complejidad requerida, deberán modificarse de manera periódica y podrán utilizarse varios sistemas complementarios (doble factor de autenticación).

4. Las credenciales de acceso serán de uso personal e intransferible, por lo que los usuarios las deberán proteger confidencialmente. En particular, se deberá evitar el almacenamiento escrito o en soporte digital no encriptado de la contraseña, debiendo ésta ser recordada por el trabajador. Quedará absolutamente prohibida su revelación o cesión a cualquier otra persona sin la autorización expresa del Ayuntamiento de Huesca.

5. En los supuestos en que el trabajador tuviera la certeza o sospechara que alguien está utilizando sus credenciales o éstas han sido comprometidas por un acceso indebido a sus dispositivos, deberá comunicarlo inmediatamente al Servicio de Nuevas Tecnologías y se le repondrán.

Artículo 7. Normas sobre Confidencialidad y Protección de Datos Personales

1. Los usuarios única y exclusivamente podrán utilizar aquellos datos a los que tenga acceso en virtud de sus funciones para dar cumplimiento a sus obligaciones laborales o políticas, quedando expresamente prohibida cualquier otra utilización.

2. Los usuarios que intervienen en cualquier fase del tratamiento de datos personales o información confidencial estarán obligados al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continuarán incluso después de finalizar su relación funcional, contractual o política con el Ayuntamiento de Huesca.

3. No se podrá borrar, destruir, dañar, alterar o modificar cualquiera de los datos personales o información confidencial sin la autorización expresa del Comité de Seguridad de la Información, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

4. Deberán respetarse los derechos de autor y la propiedad intelectual. En consecuencia, estará estrictamente prohibida la copia no autorizada de material protegido por derechos de autor (por ejemplo, gráficos de páginas web, archivos de



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

sonido, clips de películas, marcas comerciales, software y logotipos), incluida, entre otras cosas, la digitalización y distribución de fotografías de fuentes con derechos de autor y la instalación de software protegido por derechos de autor para el que el Ayuntamiento de Huesca no tenga licencia activa.

5. No se permitirá realizar copias, transmisiones, comunicaciones de los datos personales o de información confidencial, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas. Esta prohibición incluirá la visualización directa, presencial o remota de información confidencial o datos personales.

6. No se permitirá divulgar información relativa a procedimientos de adjudicación de contratos públicos, ya sea en un procedimiento de adjudicación en curso o en procedimientos de adjudicación ulteriores.

7. Los usuarios almacenarán la información confidencial y los datos personales en las aplicaciones informáticas o en las carpetas en servidores locales o en la nube, autorizados por el Comité de Seguridad de la Información, en donde se habilitará, entre otras medidas, copias de seguridad periódicas de datos. Los usuarios, por tanto, evitarán almacenar información confidencial o datos personales en:

- a) Plataformas TI municipales no habilitadas para ello, como ordenadores personales o portátiles, smartphones, dispositivos de almacenamiento externo (memorias USBs, discos externos) y otros dispositivos móviles, salvo autorización expresa del Ayuntamiento de Huesca y observando las medidas de seguridad que se indiquen.
- b) Cualquier tipo de dispositivo y Plataformas TI que no sean propiedad del Ayuntamiento de Huesca, incluyendo correos electrónicos personales, servicios en la nube no autorizados, etc..
- c) Carpetas compartidas del Ayuntamiento de Huesca a las que otros usuarios no autorizados, aunque sean municipales, puedan tener acceso.

8. Cuando el usuario tenga autorización expresa para almacenamiento de información confidencial y/o datos personales en dispositivos sin protección, como PCs, ordenadores portátiles, smartphones, tabletas, discos externos o USBs de memoria, o su envío a través de correo electrónico corporativo, almacenamiento en la nube u otros sistemas de comunicación, deberán cifrar, mediante el método aprobado por el Comité de Seguridad de la Información, toda la información confidencial o datos personales antes de almacenarla o enviarla. La clave o contraseña de descifrado deberá enviarse utilizando un canal diferente al que contenga la información cifrada (como SMS, mensajería instantánea o llamada telefónica), siempre que dicho canal esté autorizado por el citado Comité de Seguridad.



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

Artículo 8. Normas referidas a los puestos de trabajo

1. Los usuarios evitarán mostrar en las pantallas de sus dispositivos información confidencial y datos personales a personas no autorizadas.

2. Cuando el responsable del puesto de trabajo lo abandone, bien temporalmente, o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida el acceso o la visualización de su contenido mediante un protector de pantalla que impida la visualización de los datos. Para reanudar el trabajo, será necesaria la introducción de una contraseña que desactive el protector de pantalla.

3. Los puestos de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad, así como las pantallas, impresoras y cualquier otro dispositivo conectado al puesto de trabajo y desde el que sea posible tener acceso a datos de carácter personal.

4. En relación con la documentación en soporte papel, el trabajador deberá, una vez finalizadas sus tareas, archivar cualquier soporte, como documentos, fichas, discos, u otros que contengan datos personales, y proceder a guardarlos en su lugar de almacenamiento correspondiente, o en su caso, destruir la documentación si se trata de copias temporales.

5. Queda expresamente prohibido sacar cualquier Plataforma TI fuera del lugar de trabajo habitual, a menos que se esté autorizado para ello.

Artículo 9. Incidencias de seguridad

1. Los usuarios tendrán la obligación de comunicar con prontitud cualquier incidencia, anomalía, error o fallo que detecten en relación con el uso de información confidencial, tratamiento de datos personales, ciberincidentes u otras afecciones a Plataformas TI al Servicio de Nuevas Tecnologías mediante el procedimiento habilitado para ello. La información relacionada con las ciberincidencias deberá considerarse información confidencial, según la Normativa de Clasificación y Tratamiento de la Información, y los usuarios no estarán autorizados a revelar detalles de éstas a otros usuarios o personas externas

2. Se registrarán todas las actuaciones relacionadas con la gestión de incidencias según el siguiente detalle:

a) Reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

b) Deberán guardarse las evidencias cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

c) Mediante el análisis de incidencias, se revisará la determinación de eventos auditables.



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

3. El responsable de seguridad deberá comunicar las incidencias de seguridad detectadas a la Oficina de Seguridad y Protección de Datos para registrar la correspondiente desviación en el Sistema de Gestión de Seguridad de la Información.

4. Los usuarios podrán solicitar una autorización de una excepción al cumplimiento de estas normas al Servicio de Nuevas Tecnologías si creen que una excepción permanente o temporal a estas restricciones es aplicable durante el transcurso de sus funciones y deberes legítimos. Estas excepciones podrán ser validadas por el Comité de Seguridad de la Información cuando su importancia así lo requiera.

Artículo 10. Uso del correo electrónico corporativo y otros canales de comunicación

1. El correo electrónico corporativo proporcionado por el Ayuntamiento de Huesca es propiedad de éste y no se permitirá su utilización para otros fines que no sean los estrictamente profesionales. El usuario no podrá utilizar el correo para enviar datos personales u otra información confidencial, si esta comunicación no entrara dentro de sus tareas profesionales. En el caso de envío de información confidencial deberá ser cifrado mediante el método aprobado por el Comité de Seguridad de la Información.

2. Los usuarios solo podrán utilizar los canales de comunicación aprobados por el Comité de Seguridad de la Información para intercambio de información confidencial o datos personales. En particular, no podrán utilizarse canales de propósito general como Whatsapp, Instagram u otros para ese tipo de comunicaciones.

3. Los usuarios deberán tomar todas las medidas de precaución a su alcance para evitar el “phishing”; en particular, no deberán confiar, por defecto, en los mensajes de correo electrónico y/o llamadas telefónicas desde los que alguien, solicite, sin limitación: abrir un archivo adjunto desconocido, cualquier información confidencial o sus credenciales, actualizar los números de cuenta bancaria de proveedores, la instalación de software o una conexión remota al dispositivo de los usuarios, para ponerse en contacto con terceros (por correo electrónico, fax o teléfono), y seguir sus instrucciones, o hacer o aprobar transacciones monetarias.

Artículo 11. Uso personal de Plataformas TI y uso de dispositivos personales en el ámbito municipal

1. El uso personal de las Plataformas TI estará permitido, únicamente de manera limitada y ocasional, cuando dicho uso no afecte al rendimiento laboral de los usuarios, no perjudique en modo alguno al Ayuntamiento de Huesca, no infrinja ninguna disposición de la relación funcional, contractual o política del usuario con el Ayuntamiento y no haga que el usuario incumpla obligaciones



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

legales. El Ayuntamiento de Huesca no se hará responsable de los contenidos privados y datos personales que los usuarios almacenan o transmiten a través de las Plataformas TI.

Estará estrictamente prohibido cualquier uso personal de las siguientes plataformas TI: correo electrónico u otros canales de comunicación corporativos, y el software y las aplicaciones informáticas de uso municipal,

2. Estará prohibido conectar dispositivos que no sean del Ayuntamiento (incluidos, entre otros, dispositivos personales o de terceros) a la red corporativa municipal. Queda prohibido utilizar dispositivos personales para almacenar información confidencial o datos personales. En particular, no se podrá almacenar el correo electrónico corporativo en dispositivos personales, aunque sí podrá accederse desde éstos a la versión en la nube del correo.

Artículo 12. Contratación de Servicios y Plataformas TI

La contratación o el uso de una nueva Plataforma o Servicio TI (incluidos los servicios en la nube) que requiera cualquier departamento del Ayuntamiento de Huesca se llevará a cabo desde el Servicio de Nuevas Tecnologías o, en todo caso, requerirá la autorización previa por escrito de este servicio que llevará a cabo la evaluación de seguridad correspondiente para verificar su elegibilidad.

Artículo 13. Manipulación de Plataformas TI

Estará prohibido expresamente cualquier manipulación de las plataformas TI con el objeto de:

1. Intentar u obtener acceso no autorizado o ilegal a recursos informáticos u otros dispositivos, información confidencial y datos personales. Esto incluirá, sin limitación, iniciar escaneos de vulnerabilidades y descargar, almacenar o utilizar herramientas de piratería. El personal designado por el Servicio de Nuevas Tecnologías es el único autorizado para probar vulnerabilidades y controles de seguridad en las Plataformas TI.

2. Omitir o permitir que otros omitan los controles de seguridad para acceder a Plataformas TI o intentar alterar archivos, soluciones antimalware, la red privada virtual, softwares de seguridad, configuraciones, o cualquier otra funcionalidad de los sistemas del Ayuntamiento incluyendo, sin limitación, los archivos de registros de auditoría que rastrean la actividad en el sistema.

3. Instalar software que no haya sido previamente autorizado por el Servicio de Nuevas Tecnologías y, en su caso, por el Comité de Seguridad de la Información o que no esté relacionado con las funciones y deberes de los usuarios en el Ayuntamiento. El software autorizado deberá utilizarse de acuerdo con los acuerdos de licencia del proveedor de software. El Servicio de Nuevas Tecnologías se reservará el derecho de supervisar cualquier dispositivo proporcionado a los usuarios con el fin de verificarlo.



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

4. Realizar cualquier monitorización de datos o tráfico en la red, prueba de seguridad o intrusión o vulnerabilidad sin autorización previa del Servicio de Nuevas Tecnologías.

5. Alterar, destruir, reconfigurar o borrar cualquier elemento de los recursos TI cuando dicha actividad no esté incluida en las funciones de los usuarios o dañe o destruya intencionalmente la integridad de cualquier información o software del Ayuntamiento que resida en su Plataforma TI.

6. Cualquier actividad que de alguna manera amenace la seguridad de la red del Ayuntamiento mediante la publicación, transmisión, vinculación o distribución de cualquier información o software que contenga un malware u otro componente dañino, destructivo o disruptivo.

CAPÍTULO III. INCUMPLIMIENTO DE LA NORMATIVA

Artículo 14. Supervisión del Ayuntamiento de Huesca

El Ayuntamiento de Huesca verificará el cumplimiento de esta normativa a través de:

– Cuando existan sospechas razonables de incumplimiento de esta normativa, el Servicio de Nuevas Tecnologías podrá revisar la información transmitida a través de los sistemas del Ayuntamiento accediendo al dispositivo de los usuarios con el fin de garantizar la seguridad de la información confidencial y los datos personales, con o sin previo aviso al usuario y siempre respetando las leyes y regulaciones aplicables.

– El Ayuntamiento podrá revocar los certificados utilizados e instalados en los dispositivos de los usuarios y recuperar las claves de cifrado cuando exista causa justificada para acceder al contenido del correo corporativo, archivos o bases de datos y descifrar la información.

– Se realizará supervisión automática de las comunicaciones de los usuarios a través de recursos informáticos para detectar y proteger al Ayuntamiento de ciberincidencias e investigar las desviaciones y problemas de rendimiento del sistema. Las comunicaciones cifradas se podrán descifrar para revisar automáticamente la seguridad del contenido transmitido o evitar violaciones de datos personales. Estas acciones incluirán, entre otras, determinar si un usuario infringe esta normativa o, según sea necesario, garantizar que el Ayuntamiento no quede sujeto a reclamaciones de ilegalidad o mala conducta.

– Las conexiones a Internet y los archivos transmitidos a dispositivos o servicios externos se supervisarán y registrarán. Este seguimiento del uso de Internet será únicamente para garantizar que esta normativa y otras políticas se cumplan y que el Ayuntamiento y sus usuarios actúen legalmente. Estos registros incluirán información de qué Plataforma TI se haya accedido y por quién. También se comprobarán automáticamente de forma regular para detectar ciberataques, violaciones de datos personales y accesos a sitios web inaceptables.



AYUNTAMIENTO
DE HUESCA

Secretaría
Exp: 6804/2024

Artículo 15. Infracciones de esta normativa

1. En el supuesto de que algún usuario no observara alguno de los preceptos señalados en este reglamento, sin perjuicio de las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tuviera asignados, previa instrucción del procedimiento administrativo correspondiente.

2. En el caso del personal funcionario, laboral o eventual, los actos irregulares también serán objeto de los expedientes disciplinarios previstos en la legislación vigente para cada tipo de personal.

3. Si el incumplimiento de las normas se ha producido por parte de algún miembro político de la Corporación municipal, el Ayuntamiento de Huesca adoptará las medidas previstas en el estatuto aplicable a los miembros de las entidades locales.

4. En el caso de personal de empresas contratistas del Ayuntamiento de Huesca, el incumplimiento de esta normativa podrá derivar en la resolución del contrato, siguiendo el procedimiento establecido al efecto en la legislación de contratos del sector público.

DISPOSICIÓN DEROGATORIA

Quedan derogadas todas las normas del Ayuntamiento de Huesca que se opongan, contradigan o resulten incompatibles con las disposiciones de este reglamento.

DISPOSICIÓN FINAL. PUBLICACION Y ENTRADA EN VIGOR

De conformidad con lo dispuesto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, una vez que el acuerdo de aprobación de este reglamento tenga carácter definitivo, se publicará el texto íntegro del mismo en el Boletín Oficial de la Provincia de Huesca, entrando en vigor a los quince días hábiles desde la publicación del texto de la misma en dicho Boletín.