DIPUTACIÓN DE VALLADOLID

Directrices y Política de Uso y Buenas Prácticas en la utilización de los Sistemas de Información y la Red Corporativa de la Diputación de Valladolid

DIPUTACIÓN DE VALLADOLID

Índice de contenidos

1. Introducción.

La introducción de las Tecnologías de la Información y la Comunicación (en adelante TIC) dentro del ámbito de la Administración Pública está marcando el ritmo del cambio de las Administraciones Locales a medio y largo plazo. La Diputación Provincial de Valladolid se halla, pues, ante un escenario de cambio y consolidación de un proceso de transformación digital, basado en la innovación para la mejora continua, tanto de la propia institución como de los servicios que presta a los ayuntamientos de la provincia y a la sociedad en general.

En este escenario, la Diputación Provincial de Valladolid tiene que ser capaz de adaptarse a estos cambios en pos de ofrecer un servicio de calidad. En los últimos años, la introducción y utilización de las TIC ha supuesto para los empleados tener a su disposición una serie de recursos tecnológicos que facilitan enormemente la realización de su actividad laboral, pero que, simultáneamente, conllevan una responsabilidad en su buen uso y aplicación diaria.

Los usuarios de los Sistemas de Información y de la Red Corporativa de la Diputación de Valladolid son responsables de no abusar de estos recursos, respetando los derechos de los otros usuarios, la integridad del sistema y de los recursos físicos así como las leyes y regulaciones vigentes.

Por todo ello, se hace necesario establecer un modelo homogéneo de utilización racional y eficiente de estas tecnologías, con el objetivo de mejorar la gestión administrativa, lo cual se traducirá en una mejor prestación de servicios a los ciudadanos y Ayuntamientos de la provincia. Además, es muy importante establecer directrices y recomendaciones para prevenir usos y prácticas abusivos o incorrectos de los recursos tecnológicos públicos y, especialmente, todos aquellos riesgos que afecten a la seguridad de los sistemas de información, las redes de comunicación y la información contenida en bases de datos y archivos, preservando la debidas garantías de legalidad y procurando la máxima eficacia y eficiencia en la utilización de equipos, aplicaciones, sistemas y servicios.

El presente documento pretende recoger formalmente las directrices y política de uso de los sistemas y equipos tecnológicos así como de las redes de comunicaciones y establecer una serie de obligaciones, buenas prácticas y pautas de comportamiento que deben conocer y tener presente los empleados públicos de la organización. Este documento debe servir como referencia y será susceptible de ir adaptándose y evolucionando con el paso del tiempo para incluir planes, medidas y acciones que incidan en los siguientes ámbitos:

- Sistemas para el tratamiento de la información.
- Redes de comunicación y transmisión de datos.
- Sistemas para la automatización de departamentos.
- Protección y seguridad de los datos y medios informáticos.

2. Objetivos.

Los objetivos que se busca conseguir a través de la difusión del documento de Directrices y Políticas de Uso y Buenas Prácticas en la utilización de los Sistemas de Información de la Red Corporativa de la Diputación de Valladolid, son los siguientes:

- Facilitar el máximo aprovechamiento de los medios tecnológicos en la actuación de la Diputación de Valladolid.
- Asegurar la protección de los derechos de los ciudadanos en sus relaciones con la Administración, de las personas que tienen acceso a los recursos tecnológicos de la Diputación de Valladolid así como la confidencialidad de la información, protegiendo el derecho a la intimidad.
- Proteger los sistemas de información, y los datos que contienen, de los riesgos derivados de manipulaciones incorrectas o inadecuadas de los usuarios.
- Mejorar los servicios que la Diputación de Valladolid presta a los ciudadanos, propiciando una gestión eficiente de los procesos incluidos en los sistemas de información y redes de comunicaciones con las que trabaja.
- Garantizar que las herramientas que la Diputación de Valladolid entrega a sus empleados se utilicen para el trabajo y funciones que le han sido encomendadas, evitando usos indebidos que pongan en riesgo la seguridad de los sistemas.

3. Ámbito de aplicación

3.1. Agentes

El contenido de este documento será de aplicación para todo el personal de la Diputación Provincial de Valladolid, cualquiera que sea el nivel o función que ejerza, que haga uso de los Recursos Tecnológicos Corporativos. También se aplica a cualquier otro personal vinculado a la organización o a cualquier otra entidad externa que haga uso de los recursos tecnológicos de la Diputación.

3.2. Recursos tecnológicos

Se incluyen aquí las redes de comunicaciones a las que esté conectada la Diputación de Valladolid y los servicios que se presten sobre ellas así como todos los sistemas de información corporativos, ya sean individuales o compartidos y estén o no conectados a la Red Corporativa de la Diputación de Valladolid.

También se aplica a todos los equipos (estaciones de trabajo, PC's y servidores) e infraestructura de comunicaciones que sean propiedad o estén administrados por la Diputación de Valladolid, así como aquellos equipos que se conecten a través de una extranet a la Red Corporativa de la organización. Todo esto incluye terminales, ordenadores personales, estaciones de trabajo, servidores y periféricos asociados, así como el software, independientemente de que se use para gestión administrativa, económica u otros.

3.3. Políticas específicas

El presente documento es un marco que define unas directrices y política global de uso para todos los recursos tecnológicos. De forma específica se podrán articular dentro de este marco directrices, políticas y recomendaciones de buen uso de servicios e infraestructuras, como pueden ser:

- Servicios telemáticos (correo electrónico, Web, multimedia, etc.).
- Buen uso de la infraestructura de redes y del acceso a Internet.
- Acceso a servidores con datos de carácter personal.
- Incidencias de seguridad.
- Firma electrónica y certificación digital.
- Uso de extranet y servicios vinculados a ella.
- Contraseñas y Seguridad de la Información

Cuando sea necesario el uso de infraestructuras de red externas, las políticas de estas instituciones serán de aplicación en la Red Corporativa de la Diputación.

3.4. Aspectos legales

Son de aplicación las leyes y normativa españolas, así como las que dimanen de la Unión Europea, en relación con protección de datos personales, propiedad

intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto.

4. Definiciones.

A los efectos del presente documento se entenderá por:

- Diputación de Valladolid: Todos los servicios dependientes de la Diputación y de sus Organismos Autónomos y Sociedades.
- Redes de comunicación: Infraestructura de telecomunicación accesible para los usuarios para acceso a la Red Corporativa como de acceso a la Red Provincial, correo electrónico o cualquier otro instrumento de transmisión telemática o de acceso a la información mediante la conexión de medios informáticos que sean propiedad o estén bajo supervisión de la Diputación.
- Red Corporativa: Red formada por todas las Áreas y edificios de la Diputación de Valladolid.
- Red Provincial: Red constituida por la Red Corporativa más las redes de los Ayuntamientos, Mancomunidades y otras entidades dependientes de las Administraciones Locales de la provincia de Valladolid.
- Usuarios: Toda persona física que tenga autorizado el acceso a la Red Corporativa y/o la Red Provincial. Esta autorización, en lo referente a altas, traslados y bajas, será visada por el Responsable del Área afectada o, en su defecto, de los Servicios correspondientes.
- Responsable Administrativo: Es el responsable del departamento donde están instalados los equipos informáticos. Esta responsabilidad se limita a autorizar la instalación de los mismos, quién puede utilizarlos y qué uso se hace de ellos. Normalmente el responsable Administrativo es el Responsable de Área o Servicio correspondiente o la persona en quien delegue.
- Responsable de Sistemas: Es el responsable de la gestión y administración de los equipos tecnológicos y de supervisar el cumplimiento de las directrices y política de uso de los mismos.
- Responsable de seguridad: Será quien se debe encargar de dirigir las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma.
- Recursos tecnológicos: Todos los medios de cualquier naturaleza, físicos, lógicos, que intervienen en los sistemas de información y en las redes de comunicaciones (firewall, router, switch, servidor, ordenador, escáner, impresora, sistema operativo, software y aplicaciones, etc.)
- Aplicación informática: Programa o conjunto de programas informáticos, necesarios para el desarrollo de las funciones de los usuarios, que tienen por objeto el tratamiento electrónico de la información. En esta definición se incluyen tanto las verticales (aplicaciones propias de la gestión), como las horizontales (software de tipo general como ofimática, correo electrónico, etc.).

5. Directrices para la utilización de recursos tecnológicos y acceso a servicios electrónicos

5.1. Utilización de los equipos informáticos.

- La Diputación de Valladolid pondrá a disposición de los usuarios los medios y equipos informáticos para el cumplimiento de sus obligaciones laborales. En consecuencia, dichos equipos informáticos no estarán destinados al uso personal o extraprofesional de los usuarios y éstos no gozarán del uso privativo de los mismos.
- Los usuarios deberán destinar los equipos informáticos de que sean provistos a usos compatibles con la finalidad de las funciones del servicio al que se encuentren adscritos y que correspondan a su trabajo.
- Los usuarios deberán cuidar los equipos informáticos que les sean facilitados, sin alterarlos ni modificarlos.
- Los usuarios son responsables del buen orden de los equipos informáticos, cables y conexiones con periféricos y otro equipamiento.
- Los usuarios no tienen permitido conectar a los equipos informáticos que se les provea otros equipos distintos de los que tengan instalados, ni modificar sus funcionalidades.
- Los usuarios en ningún caso podrán acceder físicamente al interior de los equipos que tengan asignados para el ejercicio de sus funciones; sólo personal autorizado por el Servicio de Informática podrá hacerlo para labores de reparación, instalación o mantenimiento.
- Los usuarios sólo podrán usar equipos que estén directamente especificados por la Diputación.
- Los usuarios deberán abstenerse de manipular los mecanismos de seguridad instalados en los equipos tanto a nivel físico (hardware) como lógico (software) así como alterar las configuraciones de gestión y mantenimiento de las que dispongan los equipos.

5.2. Utilización de las aplicaciones informáticas.

- Los usuarios deben usar exclusivamente las aplicaciones informáticas o versiones de software instaladas en sus equipos por la Diputación. En todo caso, la utilización de las aplicaciones informáticas tiene una finalidad profesional, es decir, destinada a satisfacer las obligaciones laborales y con el propósito para el que fueron diseñadas e implantadas, por lo que no pueden utilizarse con fines personales o privados.
- La Diputación de Valladolid será la responsable de configurar el sistema operativo, definir las aplicaciones informáticas de uso estandarizado y proceder a su instalación o desinstalación. Sólo tras autorización expresa, dada las características o naturaleza de las aplicaciones informáticas, podrán

los usuarios efectuar directamente su instalación. En el caso de necesitar, para un puesto concreto, un software determinado que no forme parte de las aplicaciones Corporativas, el Responsable del Área o del Servicio afectado autorizará su instalación por parte del personal técnico del Servicio de Informática, aportándose la correspondiente licencia de uso.

- Las aplicaciones informáticas están protegidas por la propiedad intelectual, por lo tanto queda terminantemente prohibido su uso, reproducción, modificación, transformación, cesión o comunicación, sin la debida autorización, con finalidad externa a la propia de la Diputación.
- Queda prohibida cualquier actuación que pueda tener consideración de provocadora o intimidatoria en el trabajo; así, debe excluirse la instalación o visualización de salvapantallas, fotos, vídeos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que atenten contra la dignidad de la persona.
- Los usuarios están obligados a cumplir las medidas de seguridad diseñadas por la Diputación, así como las prevenciones que al efecto se establezcan. Por tanto, no podrán desactivar los programas antivirus ni sus actualizaciones; tampoco podrán introducir voluntariamente programas, virus, macros o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar alteración o daño en los recursos informáticos de la Diputación de Valladolid o en los de terceros.
- El acceso a la red está protegido, para todos los usuarios, por una identificación y una contraseña. Tendrá un periodo de validez determinado por el Servicio de Informática según las necesidades que se detecten. La contraseña sólo es conocida por el usuario (ni siquiera los administradores de la red pueden conocerla) y es responsabilidad suya mantenerla en secreto y cambiarla según la solicite el sistema. Las contraseñas nuevas deben ser distintas a las utilizadas. Esta contraseña es garantía de acceso para el usuario y si se desprende un problema o mal uso de las herramientas (según lo descrito en este documento) será por una mala utilización de la contraseña y, por tanto, responsabilidad del usuario.
- Los usuarios están obligados a utilizar, para la prevención de la entrada en los sistemas informáticos de cualquier elemento destinado a alterar o dañar los recursos informáticos, exclusivamente los programas antivirus y sus respectivas actualizaciones u otros sistemas de seguridad que sean instalados por la Diputación.

5.3. Utilización de la información incorporada a los sistemas.

- La información albergada en los servidores de la Diputación, o que circule a través de su red mediante elementos de comunicación o transmisión que sean de su propiedad o le hayan sido confiados, tiene carácter confidencial. Las Áreas y Servicios generadores de la información serán responsables de la misma y del cumplimiento de lo señalado en la Ley Orgánica de Protección de Datos (LOPD). Asimismo, serán responsables de autorizar los permisos y

niveles de acceso a la información que serán asignados por el Servicio de Informática.

- Los usuarios están obligados a proteger la información evitando envíos no autorizados al exterior, incluyendo tanto el acceso como la visualización de la misma. Una especial consideración de confidencialidad, en función de lo determinado en la LOPD, corresponde a ficheros o información que contengan datos de carácter personal.
- El conocimiento por los usuarios de la información reseñada en el punto primero de este apartado no confiere derecho alguno en cuanto a posesión, titularidad o derecho de copia de la misma, por lo que queda expresamente prohibido la extracción total o parcial en cualquier medio, informático o no, de la información sin la autorización documentada por parte del responsable de ésta. Según lo indicado anteriormente, su uso debe ser estrictamente oficial y profesional.
- Los usuarios con acceso a información y datos deben usarlos únicamente para las operaciones para las que fueron generados e incorporados, sin destinarlos a otros fines o incurrir en actividades que puedan considerarse ilícitas o ilegales. Asimismo, sólo deben acceder a aquellos datos y recursos que precisen para el ejercicio de las funciones que les correspondan, y efectuar sólo los tratamientos que sean precisos para el cumplimiento de los fines del servicio al que estén adscritos. Para ello, se dispondrá de perfiles de acceso y una segmentación conveniente, tanto de los usuarios como de las necesidades de información.
- Los usuarios están obligados a proteger la información y los datos a los que tienen acceso. Esta protección debe prevenir el empleo de operaciones que puedan producir una alteración indebida, inutilización o destrucción, robo o uso no autorizado; en suma, cualquier acción que pueda dañar los datos, aplicaciones informáticas y documentos electrónicos propios de la Diputación.
- Los usuarios, conforme a las instrucciones que reciban, utilizarán los medios o programas de salvaguarda que les facilite la Diputación de Valladolid con la finalidad de garantizar la integridad y seguridad de los equipos informáticos, de las aplicaciones informáticas y de la información que contengan. En cualquier caso, no intentarán descifrar claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervengan en los procesos telemáticos. La información deberá residir únicamente en los servidores asignados al usuario por del Servicio de Informática y será responsabilidad de éste la obtención de las copias de respaldo y su custodia, para lo que la Diputación de Valladolid suministrará al Servicio de Informática las ubicaciones adecuadas a tal fin. La información que resida en el almacenamiento del puesto de trabajo no es responsabilidad del Servicio de Informática y no tendrá copias de respaldo.
- Los usuarios están obligados a notificar cualquier incidencia o anomalía en el uso de los medios informáticos que detecten: pérdida de información, de listados, acceso no autorizado, uso de su identificador de usuario o de su contraseña, introducción de virus, recuperación de datos, desaparición de

soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.

- Cualquier fichero que se introduzca en la Red Corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a la propiedad intelectual, el control antivirus y la protección de datos de carácter personal.
- Se evitará la ubicación de ficheros que contengan datos de carácter personal en los equipos de los usuarios. Los usuarios sólo podrán crear ficheros temporales que contengan datos de carácter personal cuando sean necesarios para el desempeño de sus funciones; en todo caso, deberán ser eliminados cuando hayan dejado de ser útiles para la finalidad para la que fueron creados.
- Toda salida de información que contenga datos de carácter personal, sea en soportes informáticos, correo electrónico, portátiles, etc., sólo podrá realizarse por personal autorizado formalmente por el responsable del fichero, siempre cumpliendo la normativa vigente que garantiza los niveles de protección. Existirá un registro donde queden anotadas las autorizaciones.
- Los usuarios autorizados a manejar soportes que contengan datos de carácter personal deben guardarlos en lugar seguro, especialmente finalizada la jornada laboral.
- Si un usuario finaliza su relación funcionarial o laboral con la Diputación, o se traslada de puesto de trabajo, deberá dejar, sin producir perjuicio alguno, todas las aplicaciones informáticas, ficheros, información, datos y documentos electrónicos que haya utilizado en su actividad profesional a disposición de su responsable inmediato para que, con la colaboración del Servicio de Informática, se pongan a disposición del nuevo usuario que los necesite.
- Finalizada la relación funcionarial o laboral con la Diputación, el trabajador dejará de tener acceso a los equipos informáticos y a la información incorporada a los mismos, debiendo devolver aquellos que se encuentren en su posesión. Seguirá obligado a mantener la máxima reserva y confidencialidad, no sólo de la información y documentos, sino también de las claves, análisis y aplicaciones informáticas. La responsabilidad de comunicar esta nueva situación al Servicio de Informática corresponderá al Área responsable.

5.4. Acceso a la información.

- Todo usuario con acceso a un sistema de información dispondrá de una única autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y contraseña. Estos permitirán una identificación individual, evitándose registros duplicados o múltiples.
- Los usuarios deben custodiar convenientemente su identificador de usuario y su contraseña, sin proceder a su revelación o puesta al alcance de terceros.

Serán responsables de toda la actividad relacionada con el uso de su acceso personal autorizado.

- Si los usuarios sospechan que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona deberá proceder inmediatamente al cambio de contraseña y a notificar la correspondiente incidencia.
- Los usuarios no deben intentar obtener otros derechos de acceso al suyo personal, ni utilizar ningún otro acceso autorizado que corresponda a otro usuario, aunque disponga de la autorización de éste.

5.5. Acceso a las redes de comunicación.

- La conexión de los usuarios a las redes de comunicación será facilitada por la Diputación.
- Queda prohibido conectarse a la Red Corporativa por otros medios distintos a los definidos y administrados por la Diputación.
- Queda prohibido conectarse a la Red Corporativa con cualquier equipo informático distinto a los instalados para tal fin por la Diputación. El personal externo que deba conectarse a los entornos corporativos desde sus equipos requerirá la autorización y, en su caso, la supervisión del responsable de los sistemas informáticos.
- La Red Wifi está destinada a la mejora de cobertura en los edificios de de la Red Corporativa de la Diputación así como a la prestación de determinados servicios a usuarios externos. Por ello, se distinguirán dos tipos de acceso:
    - Usuario Invitado: Accede bajo unas condiciones que deberá aceptar y que se encuentran bajo una política de uso mucho más restrictiva, pudiéndose establecer límites en la utilización del acceso (tiempo, velocidad…), suspender el servicio o bloquear ciertos comportamientos, acceso a ciertos servicios o dominios para proteger la Red Corporativa de fraudes o actividades que atenten contra las legalidad.

      El administrador de sistemas, puede limitar este servicio en cualquier momento y por cualquier motivo, incluyendo emergencias, fallo del enlace, problemas en equipos de red, interferencias o fuerza de la señal. Asimismo la Diputación, no se responsabiliza por datos, mensajes o páginas perdidas, no guardadas o retrasos por interrupciones o problemas de rendimiento con el servicio ofrecido a invitados.
    - Usuario empleado público: El acceso es similar al acceso desde un puesto de trabajo cableado. Tiene los mismos requisitos y obligaciones de uso y de seguridad que el acceso desde cualquier puesto de trabajo con un equipo corporativo.
- NO se podrá utilizar la red WI-FI con los siguientes fines:

- Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea éste material o mensajes.
- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento. Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red. Enviar mensajes no solicitados (spam), virus, o ataques internos o externos a la Red Corporativa.
- Obtener acceso no autorizado a equipos, sistemas o programas tanto en la Red Corporativa como fuera de ella. Tampoco podrá utilizar la red WI-FI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.
- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno, o material protegido por secreto comercial o patentes.
- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.

5.6. Acceso a Internet.

- Los usuarios accederán a Internet empleando exclusivamente los medios y la red establecida a tal efecto por la Diputación de Valladolid, quedando expresamente prohibida cualquier otra modalidad de acceso a la red, salvo autorización expresa de la Dirección de Área correspondiente.
- Las conexiones a Internet que se produzcan a través de la Red Corporativa tendrán una finalidad profesional. En este sentido, cada usuario autorizado empleará estas conexiones exclusivamente para el ejercicio de las tareas y actividades que corresponden a las funciones de su puesto de trabajo.
- No deberá accederse en ningún caso a direcciones de Internet que tengan un contenido ofensivo o atenten contra la dignidad humana. A estos efectos, la Diputación de Valladolid podrá restringir el acceso a determinados servidores de contenidos en Internet.
- Las autorizaciones de acceso a Internet se concederán de acuerdo con las funciones del puesto que desempeñe el usuario, produciéndose una segmentación de perfiles que habilite las conexiones.
- La Diputación de Valladolid, por motivos de seguridad y rendimiento de la red, podrá regular y controlar los accesos a Internet. Se podrá proceder a monitorizar las direcciones de acceso y el tiempo de conexión de los usuarios a Internet, así como la limitación de su uso en razón de las funciones que ejerza.
- La Diputación de Valladolid podrá registrar todos los accesos a servidores de la red, incluyendo, al menos, la información de direcciones de páginas

visitadas, fecha y hora, ficheros descargados, usuario y puesto desde el que se ha efectuado la conexión.

- Quedan terminantemente prohibidas la instalación de proxys por los usuarios y la manipulación de la configuración de la conexión a Internet y del navegador.
- Las transferencias de datos desde o a Internet se realizarán exclusivamente cuando lo exija el ejercicio de las funciones del puesto de trabajo. Los usuarios deberán tener en cuenta, antes de utilizar la información proveniente de la red, si dicho uso es conforme a las normas que protegen la propiedad intelectual e industrial; en caso contrario, la responsabilidad les corresponderá exclusivamente.

5.7. Utilización del Correo electrónico.

- La Diputación de Valladolid suministrará a cada usuario que lo necesite una dirección individual de correo electrónico, procediendo a instalar y configurar un cliente de correo para su utilización. El acceso a dicha cuenta de correo se efectuará mediante una clave personal.
- Los usuarios tienen prohibido el uso en las redes de comunicación de otras cuentas de correo electrónico distintas a las facilitadas por la Diputación.
- La utilización por los usuarios del correo electrónico habilitado por la Diputación de Valladolid es estrictamente profesional, es decir, para el ejercicio de las funciones propias del puesto de trabajo que desempeñen.
- Los usuarios tienen prohibido expresamente el acceso a cuentas de correo que no le hayan sido asignadas. Para que un usuario distinto pueda acceder a una cuenta de correo será preciso que el titular de ésta lo autorice por escrito, salvo los supuestos de cuentas de correo asociadas a puestos de carácter genérico.
- Los usuarios no pueden interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otros usuarios.
- Queda prohibido para todos los usuarios el uso abusivo del correo electrónico, utilizando mensajes con contenidos ofensivos o que atenten contra la dignidad humana. Asimismo, queda prohibido el envío deliberado de cualquier clase de programa o virus que puedan causar perjuicios en los sistemas de información de la Diputación de Valladolid o de terceros.
- Los usuarios tienen prohibido el uso abusivo del sistema de listas de correo para el envío de mensajes de forma masiva o piramidal.
- Con la finalización de la relación funcionarial o laboral, que habrá de ser comunicada al Servicio de Informática por el Área responsable, se interrumpirá el acceso a la cuenta de correo del usuario.

5.8. Firma Electrónica

La Diputación de Valladolid establecerá el conjunto de criterios comunes asumidos por dicha Administración y sus organismos públicos vinculados o dependientes, en relación con la autenticación y la firma electrónica, que afecta a las relaciones de esta Administración con los ciudadanos y entre sus distintos órganos, según lo previsto en la normativa vigente.

Se determinarán una serie de normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,…), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso.

6. Políticas de uso

A continuación se plantean una serie de consideraciones que pretenden regular el buen uso, disponibilidad y nivel de servicio de los recursos tecnológicos de la Diputación de Valladolid.

6.1. Sobre la integridad y disponibilidad de los recursos

Los usuarios deben respetar la integridad de los recursos y sistemas de información. Para ello se enumeran una serie de recomendaciones:

- Un usuario no debe tratar de alterar o eliminar ordenadores (hardware o configuración del SO), software o periféricos que estén asignados a otros usuarios, sin la debida autorización.
- Los usuarios no deberán entorpecer o absorber recursos compartidos de forma tal que impidan a otros realizar sus tareas de una forma eficiente. Esto incluye, al menos, lo siguiente:
    - El envío a través de correo electrónico de cartas encadenadas o mensajes excesivamente voluminosos o con muchos destinatarios, ya sean locales o ajenos a la Diputación.
    - Uso de programas que puedan saturar los servidores o las redes de la Diputación, cuando haya alternativas más eficientes o no tengan una prioridad alta. En cualquier caso, se deberá solicitar con la suficiente antelación al responsable de sistemas.
    - Modificación no autorizada de privilegios o permisos.
    - Intentos de desactivar servidores o cortar el funcionamiento de las redes.
    - Intento de realizar cualquier tipo de daño (físico o lógico) a las herramientas informáticas de la Diputación: equipos, aplicaciones, documentos, etc.
- Los usuarios no deberán intencionadamente desarrollar o usar programas cuyo objetivo sea dañar otras máquinas o acceder a recursos restringidos (malware: virus, troyanos, puertas traseras, etc.). Más aún, deberán controlar que no se les infecte su equipo con este tipo de software, para lo cual el responsable de seguridad, deberá proporcionar las herramientas y utilidades adecuadas.
- Los usuarios de la Red Corporativa no deben utilizar los enlaces de red para otros usos que no sean los permitidos o los propios necesarios para el desempeño de su actividad.

6.2. Sobre accesos no autorizados y suplantación de identidad.

Los usuarios no deben tratar de conseguir accesos a sistemas o recursos a los que no estén autorizados y tampoco permitir o facilitar que otros lo hagan.

Los usuarios deben respetar los derechos del resto de usuarios; la mayoría de los sistemas de uso compartido proporcionan mecanismos para proteger los datos e información privada de posibles consultas por parte de otros. Los intentos de saltarse estos mecanismos para conseguir accesos no autorizados a información calificada como personal supondrán una violación de esta política e incluso del marco legal.

Los administradores de sistemas que estén autorizados podrán acceder, exclusivamente por motivos de mantenimiento y/o de seguridad, a información y datos que permita detectar, analizar y seguir las trazas de una determinada sesión o conexión. En cualquier caso, el administrador de sistemas tiene el deber de guardar secreto sobre el contenido de esta información y datos, no estando autorizado a permitir que terceros puedan acceder a ellos.

En el supuesto de que una política interna expresamente lo autorice, el administrador de sistemas podrá permitir el acceso a terceros a determinados ficheros de otros usuarios, debiendo contar en todo caso, tanto con la autorización del Responsable del Área o del Servicio como del propietario de los ficheros.

- Los usuarios de los recursos tecnológicos de la Diputación no deben acceder a ordenadores, aplicaciones, datos o información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir de forma intencionada que otros lo hagan, independientemente de que el recurso (equipo, aplicación, red, datos, etc.) pertenezca o no a la Diputación.
- No está permitido realizar de forma intencionada acciones cuyo fin sea la obtención de contraseñas de otros usuarios sin el consentimiento de estos.
- Cualquier defecto o anomalía que se descubra en el sistema o en su seguridad se debe reportar con la mayor brevedad posible al responsable de seguridad, quien será el encargado de investigar y proponer soluciones al problema.
- Todo aquel usuario que haya sido autorizado a usar una cuenta mediante un sistema de usuario/clave será responsable de mantenerla en secreto y no darla a conocer a nadie más sin la autorización del administrador del sistema. Será siempre el responsable de lo que se ejecute en el sistema desde esa cuenta.
- Los usuarios deberán evitar el tener compartidos recursos (ficheros, directorios, etc.) sin los mecanismos de seguridad necesarios y disponibles en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

6.3. Sobre el uso de los servicios de comunicación y difusión de información

El correo electrónico, las listas de distribución, servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así como la difusión de información a varios interlocutores de una sola

vez. Por ello conviene tener en cuenta una serie de comportamientos a la hora de usar estos medios.

- No se deben usar estas utilidades para el envío de mensajes con contenido fraudulento, ofensivo, obsceno o amenazante.
- Las listas de distribución de correo se deben usar sólo para enviar mensajes relacionados con la finalidad de las mismas. Existirán también listas libres, que deberán observar, no obstante, lo expuesto en el punto anterior. Podemos considerar que los usuarios se han suscrito a una lista para recibir un tipo de información y en caso de que no se respetara lo anterior el resto de los suscriptores de la lista podrían quejarse de recibir información no solicitada.
- Los recursos tecnológicos no se deben usar para actividades personales que no tengan relación con las propias del desempeño laboral. En estos casos el responsable de sistemas no está obligado a prestar soporte.

6.4. Sobre uso de la infraestructura de comunicaciones

- No se podrá instalar ningún servicio telemático (Correo electrónico, Servidores Web, FTP, etc.) sin la autorización expresa del responsable administrativo y con la designación de un administrador del sistema.
- No se podrá realizar la conexión, desconexión o reubicación de equipos o cambios de configuración de los mismos sin la autorización expresa del responsable administrativo o del administrador del sistema.
- Estará prohibido la instalación de dispositivos, y tarjetas de acceso remoto, módems, RDSI, ADSL, routers o cualquier otro dispositivo de comunicaciones en ordenadores o redes sin la autorización expresa del responsable administrativo o del administrador del sistema.
- Estará prohibido la conexión de equipos de comunicaciones para intercambio de información (rutas, redes,...) entre ordenadores de las redes de la Diputación de Valladolid y otros ajenos a dichas redes.
- Estará prohibido el uso de la red y ordenadores de la Diputación para conseguir acceso no autorizado a cualquier ordenador.
- Estará prohibido instalar o ejecutar en cualquier punto de la Red Corporativa (ordenadores o software de red) programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye sniffer, escaneadores de puertos, etc.
- No se podrá facilitar a una tercera entidad acceso, a través de la Red Corporativa de la Diputación, a la infraestructura de comunicaciones propias de este organismo; es decir, no se podrá proporcionar tránsito a terceras instituciones, salvo que una política específica lo determine.
- No se podrá proceder a la destrucción, manipulación o apropiación indebida de la información que circule por la red.

- Se evitará el consumo excesivo de los recursos por parte de cualquier usuario.
- Se deberá respetar el derecho de privacidad de los diferentes usuarios de la red

La infraestructura de Red Corporativa nunca deberá ser utilizada, bajo ningún concepto, para lo siguiente:

- Transmisión de información o acto que viole la legislación vigente en el Estado Español.
- Fines privados o personales, con o sin ánimo de lucro.
- Fines lúdicos
- Fines no estrictamente relacionados con las actividades propias de la Organización.
- Creación o transmisión de cualquier tipo de información que sea ofensiva, obscena o indecente.
- Transmitir información difamatoria de cualquier tipo, ya sea contra entidades o personas
- No se podrá divulgar información que viole los derechos de propiedad intelectual.
- No se podrá usar cualquier aplicación de la cual se sepa que su uso pueda suponer una disfunción de la red.

6.5. Sobre las licencias de software y "copyrights"

Los usuarios y administradores deben respetar las condiciones de licencia y copyright del software que usen en sus equipos.

- Todo software adquirido de forma central para la Diputación (licencias campus o licencias para instalación en servidores centrales) deberá estar debidamente licenciado.
- Todo software que se use en la Diputación para fines administrativos debe estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios simultáneos. Por supuesto, podrá usarse en equipos de la Diputación software "libre" (Open source, freeware, etc.).
- Todo software que se use que esté protegido por copyrights no puede ser copiado, salvo con autorización del propietario. No se podrán usar los medios que la Diputación pone a disposición de su comunidad para copiar software protegido o romper las protecciones del mismo.
- Aparte del software, toda otra información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo o red, se debe usar de acuerdo con la legislación vigente.

- Los usuarios responderán siempre personalmente del software que haya instalado en sus equipos, así como del uso que del mismo se efectúe, y deberán cumplir con las obligaciones y requisitos que se deriven de su instalación y utilización.

En ningún caso los usuarios podrán permitir que ninguna persona lleve a cabo la instalación en sus equipos de software que no esté debidamente licenciado.

El incumplimiento de estas obligaciones por parte de los usuarios dará lugar a la aplicación de las medidas preventivas, correctivas y disciplinarias previstas en el presente documento y, en su caso, al ejercicio de las acciones legales pertinentes.

6.6. Sobre buenas prácticas medioambientales en el uso de los recursos tecnológicos

Los usuarios de recursos tecnológicos de la Diputación pueden, y deben, aplicar diferentes recomendaciones para hacer un uso más inteligente y responsable de los distintos equipos y dispositivos, reduciendo con la aplicación de estas recomendaciones su consumo de energía, prolongando la vida útil de los mismos y en consecuencia reduciendo su huella de carbono.

En relación a ORDENADORES Y MONITORES:

- Reducir la intensidad del brillo de la pantalla reduce el consumo de energía. Otra opción complementaria a la reducción del brillo es la de elegir imágenes con colores oscuros para el fondo de pantalla del escritorio, que puede llegar a consumir un 25% de energía menos en su despliegue.
- Configurar adecuadamente el tiempo de inactividad para que se activen distintos modos de ahorro de energía como la suspensión, el hibernado o el apagado.
- Apagar el monitor cuando no se esté utilizando.
- En vez de utilizar salvapantallas, la mejor opción es utilizar el modo hibernación (sleep) y/o poner un fondo fijo o la pantalla en negro.
- Utilizar regletas / enchufes inteligentes que corten el suministro para evitar consumos fantasma de ordenadores y periféricos.
- No dejar los DVD introducidos en el lector aunque no se estén usando.
- No tener muchos programas abiertos a la vez, en modo multitarea ya que ralentiza el funcionamiento del ordenador y aumenta el consumo energético.
- Desconectar los dispositivos externos del ordenador después de su uso.
- Utilizar el ordenador portátil o la CPU alejados de fuentes de calor y/o frío.

- No obstaculizar las entradas y salidas de aire del sistema de ventilación de los ordenadores, para evitar sobrecalentamientos y exceso de trabajo para los ventiladores, lo que aumenta el consumo energético.
- No recargar otros dispositivos conectados mediante USB al ordenador.

En relación a SMARTPHONES, TABLET Y SIMILARES

- Utilizar las funcionalidades y herramientas para optimizar la duración de la batería o instalar App para la gestión energética de los dispositivos.
- Instalar aplicaciones para eliminar elementos residuales.
- Gestionar la RAM y proceder a liberar espacio en la misma.
- Reducir la intensidad del brillo de la pantalla ahorra considerablemente el consumo de energía de la batería. Algunos Smartphone disponen de la opción "brillo automático", que adapta al brillo del ambiente.
- Deshabilitar recursos y servicios sin usar, como Wi-fi, Bluetooth y GPS en caso de no ser usadas. Enciéndelas cuando las necesites.
- Desactivar la actualización automática de e-mails o notificaciones de las redes sociales.
- Para ahorrar energía, es necesario desactivar las notificaciones de nuevos eventos, estatus, mensajes, etc.
- Activar modo avión en lugares con poca o ningún tipo de señal.
- Actualizar el sistema operativo para tener mejor rendimiento y ahorrar consumo de energía.
- Evitar colocar el dispositivo cerca de lugares calientes o fríos.
- Habilitar el modo hibernación.
- Cargar la batería conectado al toma corriente, no por medio de puertos USB.
- Los dispositivos no deben abandonarse conectados al cargador enchufado.
- Actualización de aplicaciones cuando se disponga de conexión wifi que realiza las descargas de forma más rápida.
- En algunos dispositivos, y algunas aplicaciones de ahorro de batería existen configuraciones de ahorro de batería para horarios específicos, normalmente los nocturnos.
- Como regla general, el flash de la cámara debería estar desactivado y conectarlo sólo cuando queramos hacer una fotografía que lo requiera.
- La sincronización de cuentas (google, Facebook, twitter, etc) debe realizarse a intervalos adecuados para reducir el número de conexiones necesarias para las sincronizaciones.

- Pensar adecuadamente en qué aplicaciones realmente necesitamos servicio de localización y nos aporta un valor añadido, dejándolo deshabilitado para aquellas en las que sea algo superfluo.
- Activar el Modo Vibración únicamente cuando estemos en ambientes donde por el ruido ambiente no podamos oír los tonos de llamada o bien donde deba guardarse silencio.

En relación a EQUIPOS DE IMPRESIÓN E IMAGEN

- Configurar impresoras en red para que sean utilizadas por un grupo amplio de usuarios.
- Utilizar las funciones programables de ahorro y eficiencia energética.
- Configurar las impresoras, copiadoras, fax y equipos multifunción para imprimir doble cara por defecto.
- Las impresoras deben configurarse por defecto para imprimir en B/N.
- Realizar la vista preliminar de un documento en pantalla con anterioridad a la impresión.
- Recurrir si es posible a la impresión de más de una página en cada hoja de papel.
- Archivar documentos y e-mails en formato pdf, en lugar de imprimirlos en papel.
- Marcar como favoritas las páginas web d nuestro interés en lugar de imprimir la información.
- Si necesitamos imprimir alguna información web, configurarla para optimizar la impresión, evitando espacios en blanco, banners y anuncios, avisos legales, etc. que ocupan normalmente varias páginas más.
- Trabajar electrónicamente en los borradores y compartirlos digitalmente.
- Introducir recordatorios y mensajes invitando a no imprimir correos electrónicos y archivos adjuntos
- Configurar el tipo de letra de los documentos para reducir el volumen de su impresión y el consumo de tinta. Según diferentes estudios, son recomendables las siguientes fuentes y tamaños: Century Gothic, Size 11, Times New Roman, Size 12, Calibri, Size 11 y Verdana, Size 11.
- Reducir los márgenes de los documentos. Se recomienda reducir dichos márgenes a 2cm, lo que aumenta la superficie de impresión a un 71%; o incluso 1,5 cm, lo que aumenta la superficie de impresión a un 80% y conlleva un notable aprovechamiento del papel.
- Reducir el espaciado entre líneas. Ponerlo en 1,0 o en 0,95 permite ganar una línea extra cada 20 líneas aumentando en un 5% la capacidad de líneas de la página.

- Igualmente el espaciado entre párrafos, espaciado posterior debe ajustarse para optimizar al máximo las páginas, siempre que permitan cumplir su función de distinguir entre los mismos.

En relación a la GESTION DE LA INFORMACION Y CORREO ELECTRONICO

- Utilizar programas de compresión de archivos para remitir documentos por correo electrónico.
- Optimizar o reducir los archivos con independencia de que se vayan a remitir por correo electrónico o no. Muchos de los archivos que guardamos no necesitan una calidad excepcional de imágenes y pueden ser optimizados o reducidos antes de guardarlo, por ejemplo en presentaciones Word, PowerPoint o pdf.
- Evitar enviar correos electrónicos pesados. Aún cuando se haya recurrido a la compresión, optimización o reducción de archivos, debe pensarse si es realmente necesario enviar estos por correo electrónico, especialmente cuando vaya dirigido a múltiples destinatarios.
- En correos masivos a listas de distribución la mejor opción es incorporar un enlace web al documento o información objeto del correo.
- Realizar una limpieza periódica de archivos y correo electrónico. Para optimizar las tareas de limpieza, se recomienda ordenar correos electrónicos o archivos por su tamaño, comenzando a eliminar los más grandes hasta llegar a los más pequeños.
- Evitar imprimir los correos electrónicos.
- Cuando se utilicen motores de búsqueda intentar realizar búsquedas refinadas para reducir el número de opciones seleccionadas.

7. Del personal con responsabilidades en los sistemas de información.

Como se ha expuesto antes, cada usuario se hará responsable del buen uso del equipamiento y la red que la Diputación pone a su disposición. Pero hay determinados recursos (servidores, aplicaciones, bases de datos, red) cuyo uso o explotación es compartido por un grupo de usuarios. Estos recursos tendrán un responsable administrativo (que asumirá competencias organizativas) y un administrador del sistema, que será nombrado por el responsable administrativo y que se encargará de las tareas técnicas de funcionamiento de los recursos en cuestión.

- Los trabajadores adscritos a puestos de trabajo que impliquen funciones de diseño, desarrollo, operación o administración de los sistemas de información y de las redes de comunicación quedarán exentos del cumplimiento de aquellas instrucciones contenidas en este documento que interfieran en su cometido. La autorización correspondiente será comunicada, por escrito, por la dirección del Servicio de Informática a los interesados, quienes se comprometerán, igualmente por escrito, a cumplir las normas de confidencialidad necesarias.
- El personal autorizado no podrá utilizar la información o los datos aprovechando sus privilegios de administración; sólo podrán acceder a ficheros ajenos previa autorización de su responsable y, exclusivamente, para el ejercicio de las funciones que le correspondan.
- El Servicio de Informática custodiará con especiales cuidados identificadores y contraseñas que den acceso a los sistemas con privilegio de administrador.
- El Servicio de Informática procurará que la información almacenada y tratada por los sistemas de información sea salvaguardada mediante copias de seguridad para la recuperación periódica de datos. Las copias de seguridad se harán diariamente, de lunes a jueves, de forma diferencial; estas copias tendrán una temporalidad semanal. Los viernes se hará una copia integral. Se gestionará una política de históricos de las copias de seguridad.
- El Servicio de Informática velará porque los soportes informáticos estén convenientemente registrados en un inventario actualizado, así como porque se cumpla escrupulosamente el control de acceso restringido a personal autorizado en los locales, edificios y recintos en que se encuentren los sistemas de almacenamiento y servidores. Si personal no autorizado para el acceso habitual, por necesidad de su trabajo, necesitara acceder a estas dependencias, deberá ser autorizado expresamente. Este acceso debe quedar registrado y documentado.
- El Servicio de Informática podrá monitorizar y registrar la actividad que se realice a través de las redes Wifi de la Diputación. Además el acceso a

Internet podrá ser filtrado y controlado no estando permitido el uso de técnicas, sistemas o aplicaciones que permitan evitar dicho control.

- El personal autorizado notificará cualquier violación de las normas de seguridad o de vulnerabilidad de los sistemas de información que detecten, no revelando en ningún caso a terceros estas debilidades, excepto a la persona autorizada que reciba el encargo de realizar los trabajos para su corrección.

7.1. La administración de los recursos globales.

El administrador del sistema deberá organizarse y realizar las acciones y esfuerzos necesarios para:

- Prevenir y evitar robos, pérdidas o cualquier daño físico a los componentes del sistema.
- Respetar todos los acuerdos y licencias relativos al hardware y software que sean aplicables al sistema.
- Tratar la información almacenada en el sistema de la forma apropiada y adoptar las precauciones y medidas para proteger la seguridad de los datos, red y equipos según lo especificado en el marco legal vigente y los compromisos adquiridos. Las medidas de seguridad se dimensionarán en función de la importancia y criticidad de los recursos que se quieran proteger.
- Dar publicidad a las distintas directrices, políticas y recomendaciones de uso de servicios.
- Garantizar los procedimientos de recuperación de la información y del sistema en los servidores bajo su responsabilidad.
- Colaborar con otros administradores de sistemas de otras entidades o redes, para resolver los problemas causados en las mismas desde máquinas bajo el dominio de la Diputación.

Para hacer cumplir esta política, el administrador del sistema debe contar con los medios necesarios (herramientas y personal) y la autorización (delegada por el órgano de gobierno correspondiente) para tomar medidas razonables que garanticen el buen funcionamiento de los recursos para la colectividad y su seguridad.

El administrador del sistema puede, temporalmente y con el consentimiento (cuando sea posible) del Responsable Administrativo o del Responsable de Seguridad, suspender los privilegios de acceso o conexión si lo estima necesario o apropiado para mantener la integridad y disponibilidad del sistema o de la red.

7.2. El Responsable de Seguridad.

Será quien se debe encargar de dirigir las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma:

- Interpretación de la política: Será responsable de la interpretación de esta política, de la resolución de los problemas y conflictos con las políticas locales o departamentales y otras situaciones especiales.
- Cumplimiento de la política: en los casos en que incurran violaciones a esta política, el Responsable de seguridad estará autorizado a trabajar en colaboración con las correspondientes unidades administrativas para su resolución.
- Control y monitorización: será el responsable de diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas y su grado de cumplimiento y ajuste a esta política.

Asumirá también todas las funciones y responsabilidades definidas para Responsables de seguridad en la normativa vigente sobre medidas de seguridad para ficheros con datos de carácter personal. Para asuntos legales derivados del incumplimiento de estas normas se consultará con la Asesoría Jurídica.

8. LAS CONSECUENCIAS DEL MAL USO DE LOS RECURSOS:

Aquellas personas que de forma reiterada o deliberada o por negligencia ignoren o infrinjan las directrices recogidas en este documento o no cumplan la política de uso, se podrán ver sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) o disciplinarias que se estimen oportunas.

En cualquier caso, será responsabilidad de los directivos de la Diputación dar la difusión necesaria a esta política para que sea conocida por todos los agentes a los que se aplica.

Ante un mal uso de los recursos, se pondrán en marcha las siguientes medidas:

- Colaboración de los usuarios: los usuarios, cuando se les solicite, deben colaborar con los administradores de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.
- Acciones correctivas y preventivas: si los responsables del sistema detectan la existencia de un mal uso de los recursos y éste procede de las actividades o equipo de un usuario determinado, pueden tomar cualquiera de las siguientes medidas para proteger a los otros usuarios, redes o equipos:
    - Notificar la incidencia al usuario o responsable del sistema.
    - Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.
    - Con el permiso del responsable de seguridad y la debida justificación, inspeccionar ficheros o dispositivos de almacenamiento del usuario implicado.
    - Informar a los superiores u órganos de gobierno correspondientes de lo sucedido.
- Medidas disciplinarias: en caso que fuera necesario, corresponderá al Órgano de gobierno competente la adopción de medidas disciplinarias hacia los usuarios infractores de esta política, una vez informado por el Responsable de seguridad.