NORMAS DE ACCESO A INTERNET

ÍNDICE

Revisión	Fecha	Motivo del Cambio
1	Enero 2016	Primera Emisión

Realizado y revisado Fdo. Fecha	Aprobado Fdo. Fecha

1. OBJETO

El objetivo de la presente norma es regular el acceso a Internet por parte de los usuarios de los Sistemas de Información de la Diputación de Soria posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

Este documento se considera de uso interno de la Diputación de Soria y, por tanto, no podrá ser divulgado salvo autorización del organismo.

2. ALCANCE

Esta Norma es de aplicación a todo el ámbito de actuación de la Diputación de Soria, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la entidad.

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

3. VIGENCIA

La presente Norma ha sido aprobada por la Diputación de Soria, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Diputación de Soria pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la Diputación de Soria.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa

4. NORMATIVA

Con el despliegue de las TIC y, en particular, con el desarrollo de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que pueden poner en peligro los sistemas de información de las organizaciones.

Para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso.

Tales medidas son:

- **Usar Internet para fines profesionales.** Internet es una herramienta más de las utilizadas por los usuarios de la Diputación de Soria. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales.

- **No visitar páginas de contenido poco ético, ofensivo o ilegal.** No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.

- **No visitar páginas no fiables o sospechosas.** Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas que se consideren sospechosas de contener código malicioso.

- **Cuidar la información que se publica en Internet.** No se debe proporcionar información sobre la organización en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno de la Diputación de Soria, sus recursos, estructura, etc.

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

- **Realizar descargas sólo si se tiene autorización.** Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque la Diputación de Soria decida no limitar técnicamente la capacidad para descargar archivos de audio o vídeo, los usuarios deberán tener en consideración que la descarga de estos archivos puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, limitarán su descarga y reproducción al ámbito estrictamente profesional.

- **No descargar código o programas no confiables.** Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Conviene que tales actividades sean acometidas, de manera exclusiva, por la Diputación de Soria.

- **Asegurar la autenticidad de la página visitada**. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad.

- **Comprobar la seguridad de la conexión**. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar http (examinando la barra de direcciones). También debería aparecer un icono representando un candado en la barra del nave-

gador. A través de dicho candado se puede obtener información sobre el certificado digital de identidad del sitio web visitado.

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

- **Utilizar herramientas contra código dañino.** El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes. Por tanto, es necesario disponer del adecuado abanico de herramientas que permitan una adecuada protección. El uso de un antivirus permanentemente actualizado es la primera de protección contra este tipo de ataques. Además de ello, es necesario configurar y usar adecuadamente cortafuegos, software específico contra programas espía (spyware), etc.

- **Mantener actualizado el navegador y las herramientas de seguridad**. Es imprescindible actualizar las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.) a las últimas versiones estables, siempre de conformidad con lo indicado y aprobado por la Diputación de Soria. Puesto que el código dañino se genera incesantemente, es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar sobre cualquier problema que se detecte en este proceso.

- **Utilizar los niveles de seguridad del navegador.** Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.

- **Desactivar las cookies**. Las cookies son pequeños programas que emplean los servidores Web para almacenar y recuperar información acerca de su s visitantes (Por ejem-

plo, quién, cuándo y desde dónde se ha conectado un usuario). Estos programas se almacenan en el ordenador del usuario al visitar una página Web, pudiendo ser desactivados usando las herramientas disponibles en el navegado.

- **Eliminar la información privada**. Los navegadores Web almacenan información privada durante su utilización, tal como el historial de navegación, cookies aceptadas, contraseñas, etc., información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.

- **No instalar complementos desconocidos**. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (plug-in, add-on, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.

- **Limitar y vigilar la ejecución de Applets y Scripts.** Los scripts son un conjunto de instrucciones que permiten la automatización de tareas. Los applets son pequeñas aplicaciones (componentes de aplicaciones) que se ejecutan en el contexto del navegador Web. A pesar de que, en general, resultan útiles, pueden ser usados para ejecutar código malicioso y, por tanto, es recomendable limitar su ejecución.