

NORMATIVA DE ACCESO A INTERNET




Diputación
de Soria

 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 2 de 12

GESTIÓN Y CONTROL DE DOCUMENTOS Y REGISTROS


ELABORADO POR:	REVISADO POR:	APROBADO POR:

FECHA	EDICIÓN	REVISIÓN	CAMBIOS REALIZADOS
01/08/2019	01		Versión inicial del documento
30/01/2020	01	02	Adaptación al funcionamiento interno

 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 3 de 12

ÍNDICE

1. Introducción.....	4
2. Ámbito de aplicación	4
3. Vigencia.....	4
4. Revisión y Evaluación	4
5. Marco Normativo	5
6. Normas previas	5
7. Motivación	5
8. Normativa	6
9. Características del acceso a Internet.....	9
9.1. Características del acceso a Internet	9
9.2. Categorización de las páginas web.....	9
9.3. Catálogo de ficheros de acceso restringido	10
9.4. Distribución de usuarios	10
9.5. Propuesta de asignación de usuarios a niveles de acceso	11
9.6. Características del acceso a Internet	11
10. Anexo A. Modelo de aceptación y compromiso de cumplimiento.....	12

 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 4 de 12

1. Introducción

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, desde las distintas sedes de la DIPUTACIÓN DE SORIA o a través de ellas, 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 del DIPUTACIÓN DE SORIA y, por tanto, no podrá ser divulgado salvo autorización del DIPUTACIÓN DE SORIA.

2. Ámbito de aplicación

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 DIPUTACIÓN DE SORIA.

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

La gestión de esta Norma corresponde a el área de informática o sistemas, que es competente para:

- Interpretar las dudas que puedan surgir en su publicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 5 de 12

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el área de informática o sistemas revisará la presente Norma, que se someterá, de haber modificaciones, a la aprobación del área de informática o sistemas de la DIPUTACIÓN DE SORIA.

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

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. Marco Normativo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- UNE-ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE-ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Documentos y Guías CCN-STIC.


6. Normas previas

Las presentes “Normas de acceso a Internet” complementan, en sus aspectos específicos, a las “Normas de uso del Sistema de Información del DIPUTACIÓN DE SORIA”, por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

7. Motivación

Con carácter general, los usuarios del DIPUTACIÓN DE SORIA dispondrán de acceso a Internet como herramienta de productividad y conocimiento, para el desempeño de su actividad profesional.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet por los siguientes motivos:

 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 6 de 12

- **Seguridad:** Debido al riesgo de infección por software dañino (virus, troyanos, etc.)
- **Volumen de tráfico externo de datos:** asegurando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias del DIPUTACIÓN DE SORIA.
- **Volumen del tráfico interno de datos:** como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- **Ética:** Finalmente, es ineludible el compromiso que el DIPUTACIÓN DE SORIA debe tener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

8. 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.

En este sentido, la medida de seguridad [mp.per.2] del ENS señala:


Deberes y obligaciones [mp.per.2].

1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
 - a) Se especificarán las medidas disciplinarias a que haya lugar.
 - b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
 - c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.
2. En caso de personal contratado a través de un tercero:
 - a) Se establecerán los deberes y obligaciones del personal.
 - b) Se establecerán los deberes y obligaciones de cada parte.
 - c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.


Por tanto, 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 de las más utilizadas por los usuarios del DIPUTACIÓN DE SORIA. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales.


 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 7 de 12

- **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 del 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 habituales de infección por código malicioso. Independientemente de que la DIPUTACIÓN DE SORIA decida o no limitar técnicamente la capacidad para descargar archivos de audio o video, 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 licencias para utilizar las aplicaciones descargadas. Conviene que tales actividades sean acometidas, de manera exclusiva, por el área de informática o sistemas.
- **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 navegador. A

 Diputación de Soria	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 8 de 12

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 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 protección contra este tipo de ataques. Además de ello, es necesario configurar y usar adecuadamente cortafuegos, software específico contra programas espía (spyware), etc.
- **Mantener actualizada 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 el área de informática o sistemas. 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 sus visitantes. (por ejemplo, quien, cuando y desde donde 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 navegador.
- **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.

	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 9 de 12

- **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.

9. Características del acceso a Internet

Por motivos anteriormente expuestos, el acceso a Internet de los empleados del DIPUTACIÓN DE SORIA se realizará atendiendo a los siguientes criterios:

9.1. Características del acceso a Internet

Se consideran puertos autorizados los siguientes:


Descripción del Puerto	Puerto autorizado
http (servicios web estándar)	p. ej. 80
https (servicio web seguro)	p. ej. 443
ftp (Servicio de transferencia de ficheros)	p. ej. 21
Servicios varios	p.ej. 30080

En el caso de existir otros servicios que requieran de puertos no estándar, se deberá comunicar a el área de informática o sistemas para su estudio y autorización, en su caso.

9.2. Categorización de las páginas web

Se detallan los siguientes grupos de acceso a las distintas categorías de páginas Web.

1	Categorías no permitidas	Anorexia, Bulimia, azar, Chat (con intercambio de ficheros), código malicioso, construcción de explosivos, drogas, encuentros, juegos, logos/ringtones, modelos, música, pagar por navegar, pornografía, erotismo, racismo, sectas, servidores P2P, violencia, listas negras.
2	Categorías no permitidas, salvo autorizaciones especiales	Anonimizadores, DNS Services, Hackers, servidores de mensajería instantánea, VoIP, Spyware.
3	Categorías permitidas	Resto de categorías determinadas por Diputación.

	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 10 de 12

9.3. Catálogo de ficheros de acceso restringido

Para minimizar los riesgos derivados de la descarga de ficheros, deberá considerarse restringido el acceso a los siguientes tipos de Ficheros:

- Multimedia: Video, audio y streaming.
- Ejecutables.
- Imágenes en disco.
- De tamaño excesivo.

9.4. Distribución de usuarios


Dentro del DIPUTACIÓN DE SORIA existen distintos niveles de usuarios, atendiendo a:

- Las categorías de los contenidos para los que tienen permiso de acceso.
- Los tipos de ficheros que tienen permiso de descarga.
- Limitación del tiempo de consulta.

Los usuarios se clasificarán en tres niveles de acceso, según la necesidad de utilización de Internet de los mismos:

Nivel de acceso	Categorías autorizadas	Limitación temporal	Descarga ficheros	Especificaciones
1	3	NO	NO	La lista blanca se creará de forma manual bajo demanda de los usuarios previa autorización del área de informática o sistemas. La lista blanca será de contenido útil para los trabajadores.
2	3	NO	Sólo MULTIMEDIA	
3	3 y 2	NO	Sólo MULTIMEDIA	Personal específicamente autorizado.

- El **nivel 1** tendrá acceso a páginas habituales sin restricción de tiempo y limitación de ficheros. Sin permiso para descargas.
- El **nivel 2** tendrá acceso a páginas habituales sin restricción de tiempo y limitación de ficheros. Descarga parcialmente permitida.
- El **nivel 3** tendrá acceso a más categorías que cualquier otro nivel. No se aplican restricciones sobre ficheros, excepto a aquellos no recomendados por considerarse peligrosos.

	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 11 de 12

9.5. Propuesta de asignación de usuarios a niveles de acceso

La asignación a un determinado nivel puede venir dada por el nivel profesional del usuario.

Ejemplo de asignación:

Tipo de usuario	Nivel de acceso a Internet
Para todo el personal del DIPUTACIÓN DE SORIA	1
Especiales: p.ej. Gabinete de prensa	2
Especiales: personal informático y/o de seguridad con responsabilidad en temas de internet	3


Cierto tipo de personal, podrán solicitar de forma motivada, el cambio de nivel de acceso a Internet de un usuario mediante comunicación electrónica a el área de informática o sistemas.

La asignación final del nivel de acceso de un usuario será determinada por el departamento de informática tras la valoración de la solicitud de acceso o de alta del usuario y teniendo en cuenta el nivel profesional del usuario.

9.6. Características del acceso a Internet

Con carácter general, los usuarios del DIPUTACIÓN DE SORIA dispondrán de acceso a Internet como herramienta de productividad y conocimiento en el desempeño de su actividad profesional, por lo que la suspensión de los derechos de acceso sólo podrá realizarse mediante solicitud motivada y siempre que obedezca a algunas de las causas de mala utilización/abuso.

La suspensión del acceso a Internet finalizará cuando las razones objetivas que dieron lugar a la misma hubieran desaparecido.

	NORMATIVA		ENS.NOR.SEG.02
	NORMATIVA DE ACCESO A INTERNET		
	N.º edición: 01	Revisión: 02	Página 12 de 12

10. Anexo A. Modelo de aceptación y compromiso de cumplimiento

Todos los usuarios de los recursos informáticos y/o Sistemas de Información del DIPUTACIÓN DE SORIA deberán tener acceso permanentemente, durante el tiempo de desempeño de sus funciones, a la presente Normativa, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, como usuario de recursos informáticos y sistemas de información del DIPUTACIÓN DE SORIA, declara haber leído y comprendido la NORMATIVA DE ACCESO A INTERNET de la DIPUTACIÓN DE SORIA y se compromete, bajo su responsabilidad a su cumplimiento.

En _____, a _____ de _____ de 20__

Organismo	DIPUTACIÓN DE SORIA
Trabajador (Nombre y Apellidos)	
DNI número	
Número de Registro de Personal	
Firmado:	

Por DIPUTACIÓN DE SORIA: <<nombre y Apellidos>>

DNI número: _____

Número de Registro de Personal: _____