Centro Informático Científico de Andalucía
CONSEJERÍA DE TRANSFORMACIÓN ECONÓMICA, INDUSTRIA, CONOCIMIENTO Y UNIVERSIDADES

JUNTA DE ANDALUCIA

NORMAS DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

NS02 - INTERNET

Fecha: 22 agosto 2019

Índice de contenido

1. OBJETIVO

1. El presente documento constituye la norma de seguridad del CICA en cuanto al uso de Internet y otras herramientas de colaboración, y forma parte del conjunto de normas de seguridad del CICA, "NS01 CICA – GENERAL".

2. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

2. El acceso corporativo a Internet es un recurso centralizado que el CICA pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.
3. El CICA velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

2.1. NORMAS GENERALES

4. El acceso a Internet deberá ser autorizado por la persona responsable del Área a la que pertenezca el usuario o usuaria, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.
5. Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
6. Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por el CICA en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del Área de Seguridad.
7. Deberá notificarse al CSU cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.
8. Se cuidará 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 CICA, sus recursos, estructura, etc.
9. Se observarán 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.
10. Sólo realizar descargas si se tiene autorización. Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque el CICA 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.

11. 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 el Área de Soporte.

12. 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.

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

14. 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.

15. Utilizar herramientas contra código dañino. El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes 3 . 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.

16. 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 el Área responsable de Microinformática. 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.

17. 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.

18. Desactivar las cookies. Las cookies son pequeños programas que emplean los servidores Web para almacenar y recuperar información acerca de sus visitantes. (Por ejemplo, *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 navegador.

19. 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.

20. 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.

21. 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.

2.2. CARACTERÍSTICAS DEL ACCESO A INTERNET

22. Por los motivos anteriormente expuestos, el acceso a Internet de los empleados del CICA se realizará atendiendo a los siguientes criterios:

2.2.1. PUERTOS AUTORIZADOS

23. Se consideran puertos autorizados los siguientes:

Descripción del Puerto	Puertos autorizados
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, 444, 8081, 8099, 8399

24. En el caso de existir otros servicios que requieran puertos no estándar, se deberá comunicar al CSU para su estudio y autorización, en su caso.

2.2.2. CATEGORIACIÓN DE LAS PÁGINAS WEB

25. En el Anexo I se ofrecen las distintas categorías de páginas Web, con su descripción.

26. Se detallan los siguientes grupos de acceso a tales categorías

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, Rosa, Sectas, Servidores P2P, Violencia, Listas negras.
2	Categorías no permitidas, salvo autorizaciones especiales:	Anonimizadores, DNS Services, Hackers, Servidores Mensajería Instantánea, VoIP, Spyware.
3	Categorías permitidas:	Resto de categorías señaladas en el Anexo I

2.3. USOS ESPECÍFICAMENTE PROHIBIDOS

27. Quedan prohibidas las siguientes actuaciones:

- 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.
- 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.
- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.
- La descarga de programas informáticos sin la autorización previa del Área de Seguridad, o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por el Área de Seguridad.

2.4. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

28. Todos los usuarios de los recursos informáticos y/o Sistemas de Información del CICA deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma de Acceso a Internet, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del CICA/ empleado de la <<EMPRESA>>], como usuario de recursos informáticos y sistemas de información del CICA, declara haber leído y comprendido la Norma de Acceso a Internet del CICA (versión __) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a _____ de _____ de 20__>>

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

Por el CICA: _____

DNI número: _____

Número de Registro de Personal: _____

3. ANEXO I: DESCRIPCIÓN DE CATEGORÍAS DE PÁGINA WEB

Categoría	Definición
Sector Público	Páginas Web de entidades de carácter público (Administraciones Públicas o sector Público Institucional), tales como Ministerios, Consejerías, Ayuntamientos, instituciones de la Unión Europea y, en general, cualquier dirección que aporte información referente a entidades de gobierno y administración de todo el mundo.
Anonimizadores	Páginas Web a través de las cuáles se evita el conocimiento por parte de terceros de las direcciones Web a las que se está accediendo.
Anorexia - Bulimia	Páginas Web dedicadas a promover e incitar la anorexia y la bulimia.
Arte y cultura	Páginas Web que aportan información relativa a las artes y las letras: museos, escultura, fotografía, literatura, etc.
Azar	Páginas Web desde donde poder acceder a casinos y bingos on line. Se incluyen en esta categoría páginas donde poder realizar todo tipo de apuestas.
Bancos y Entidades Financieras	Entidades bancarias, Cajas de Ahorro, Compañías de Seguros, etc.
Banners	Cuadros de propaganda o publicidad insertados en páginas Web.
Blogs	Páginas gratuitas donde particulares publican en Internet, diarios, experiencias, comentarios, ideas, etc.
Buscadores	Páginas Web utilizadas para realizar búsquedas de contenidos en Internet (google.com, yahoo.com, altavista.com, etc.).
Chat	Páginas Web desde donde poder comunicarse con otros usuarios, en tiempo real.
Código dañino	Software introducido intencionadamente en un sistema con propósito malicioso o no autorizado.
Construcción de explosivos	Páginas Web relativas a la fabricación y manipulación de explosivos.
Compras	Páginas Web a través de las cuales se pueden realizar compras de productos y servicios varios.
Correo Web	Páginas Web donde poder enviar y recibir correos electrónicos.
Deportes	Páginas Web relativas a equipos e información deportiva
DNS Services	Categoría que abarca los casos de conexiones de equipos desde la red interna a equipos de usuarios en Internet, vía http, a un puerto destino configurable y variable, con la peculiaridad de que en el

	equipo de Internet se puede disponer de herramientas (tales como Remotely Anywhere, por ejemplo) que permiten el control total del equipo de Internet al usuario de la red interna y por tanto tener una vía de escape, ejecutando http, ftp, etc.
Drogas	Páginas Web que incitan al consumo de drogas o facilitan contactos / lugares donde poder adquirir estupefacientes. No se incluyen paginas informativas / preventivas sobre drogas.
Economía	Páginas Web con contenidos de bolsa, banca, inversiones financieras, seguros, etc.
Educación	Páginas Web de colegios, universidades, academias y cursos de formación en general.
Empleo	Páginas Web de ofertas y demandas de empleo. Se incluyen también las Webs de "head-hunters".
Encuentros	Páginas Web a través de las cuales se puede conocer a otras personas: hacer amigos, encontrar pareja, etc.
Entretenimiento	Páginas Web de información de ocio: películas, obras de teatro, libros, restaurantes, hobbies, etc. Contenidos, en general, sobre cómo emplear el tiempo libre, excepto los contenidos que pertenecen a azar, deportes, juegos y viajes.
Foros	Páginas Web de carácter temático donde se puede participar aportando opiniones personales.
Guías y callejeros	Páginas Web donde se incluyen callejeros de ciudades, información acerca de direcciones, números de teléfono, etc.
Hackers	Páginas Web donde poder encontrar software ilegal o procedimientos asociados con su uso.
Hosting domains	Páginas Web de empresas que alberga páginas Web, donde se pueden adquirir dominios de Internet.
Info	Páginas Web que en general aportan información útil, como situación del estado de las carreteras, predicciones meteorológicas, etc.
Informática	Páginas Web con información relativa a hardware, sofware, Internet, etc.
Juegos	Páginas Web donde poder jugar "on-line" o descargar juegos de ordenador.
Jurídicas	Páginas Web que aportan información sobre temas legales.
Logos/Ringtones	Imágenes o Canciones (melodías monofónicas o polifónicas) que son descargadas por los usuarios de teléfonos móviles.
Modelos	Páginas Web donde se encuentren fotografías de modelos, total o parcialmente desnudos.

Música	Páginas Web para adquirir o descargar música o donde poder encontrar información relativa a cantantes y grupos musicales en general.
Pagar por navegar	Páginas Web que permiten ganar dinero en la red recibiendo correos, navegando por determinadas páginas, suscribiendo ofertas gratuitas, etc.
Páginas Personales	Páginas creadas en hosting especializados para ello, y que no están incluidas en otras categorías.
Pornografía	Páginas web de contenido pornográfico u obsceno. Se incluye el acceso a los chat donde se puede encontrar material de este tipo.
Erotismo	Páginas web de contenido erótico. Se incluye el acceso a los chat donde se puede encontrar material de este tipo.
Portales	Son sitios Web en los que se puede encontrar una amplia gama de contenidos: noticias, ocio, deportes, juegos, música, etc.
Prensa	Periódicos o revistas on-line.
Racismo	Páginas Web que abiertamente contengan contenidos de carácter xenófobo o inciten a comportamientos racistas o intolerantes por razón de cultura, raza, religión, ideología, etc.
Rosa	Páginas Web con contenidos relativos a personajes famosos. Además de contenidos como moda, perfumes, decoración, etc.
Salud	Páginas Web en las que se puede encontrar información de carácter divulgativo (no científico) acerca de enfermedades y sus remedios.
Sectas	Páginas Web de sectas peligrosas. No se incluirán aquellas organizaciones que, por legislación distinta entre países diferentes, sean consideradas sectas en unos países y asociaciones religiosas de pleno derecho en otras
Servidores P2P	Sitios donde se registran estos programas para dar el servicio y las páginas relacionadas con ellos.
Servidores Mensajería Instantánea	Sitios donde se registran estos programas para dar el servicio y las páginas relacionadas con ellos.
Sexualidad	Información y artículos sobre sexo, educación sexual, tendencias sexuales, etc., que no contienen pornografía.
Spyware	Páginas que contengan Spyware. Se considera Spyware al software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o consentimiento del propietario del ordenador.
Telecomunicaciones	Páginas Web que facilitan información acerca de temas de

	telefonía fija, telefonía móvil, conexión a internet, etc.
Viajes	Páginas Web de agencias de viajes, y aquellas con información turística acerca de ciudades, plazas hoteleras y medios de transporte.
Violencia	Páginas Web que abiertamente contengan contenidos de carácter violento, inciten a la violencia o hagan apología de ella.
VoIP	Voz sobre IP. Páginas desde las que se accede a aplicaciones que permiten la transmisión de voz en vivo a través de Internet utilizando los protocolos TCP IP.