COMITÉ OLÍMPICO
ESPAÑOL

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y USO DE MEDIOS

Código: PL005
Versión: 1.0
Fecha de emisión: 18/06/2019

HOJA DE CONTROL

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
1.0	Versión inicial	CROWE	15/04/2109

REVISIÓN Y APROBACIÓN:

Realizado por:	Revisado por:	Aprobado por:
CROWE	Secretaría General	Comité Ejecutivo
Fecha: 15/04/2109	Fecha: 31/05/2019	Fecha: 18/06/2019

CONTENIDO

1 OBJETO

El presente documento establece la Política de Seguridad de la Información del COE. En este sentido, cualquier persona, bien pertenezca al COE bien a otra entidad que preste un servicio a la misma, deberá conocer la presente Política y la deberá cumplir con todas y cada una de las obligaciones que en ella se establecen.

De igual forma, este documento establece la normativa para un uso correcto de los medios tecnológicos proporcionados por la entidad a los Sujetos Obligados (tal y como ha quedado definido este término en el Código Interno de Conducta) estableciendo una serie de medidas en relación con la utilización de los mismos, la salvaguarda de la información, y las funciones y obligaciones del personal que acceda a datos de carácter personal.

2 ALCANCE

La presente Política es de aplicación a los empleados de la entidad. Todos los empleados deberán asumir las obligaciones que, con carácter general, se describen en el apartado 4 del presente documento, extendiéndose las mismas a todos los Sujetos Obligados que pudieran utilizar los medios del COE.

3 DEFINICIONES

A continuación, se definen una serie de conceptos técnicos que se mencionan a lo largo del presente documento, para la mejor compresión del mismo por los Sujetos Obligados.

Anti-virus: programas cuyo objetivo es detectar y/o eliminar virus informáticos.

Applets: componente de una aplicación que se ejecuta en el contexto de otro programa, por ejemplo, en un navegador web.

Consumo masivo: uso excesivo por parte de un usuario de los recursos disponibles a su servicio, que afecta al correcto funcionamiento del resto de los usuarios.

Control ActiveX: entorno para definir componentes de software reusables de forma independiente del lenguaje de programación. Las aplicaciones de software pueden ser diseñadas por uno o más de esos componentes para así proveer su correspondiente funcionalidad.

Copia ilegal: aplicación instalada y usada que no ha sido adquirida por medios legales con su correspondiente número de licencia (código autentificador de su compra) y que supone una violación de los derechos de copyright.

Correo Spam: correo electrónico basura, o no solicitado, no deseado o de remitente no conocido (correo anónimo). Habitualmente de tipo publicitario, son generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

Directorio activo: término que usa Microsoft para referirse a su implementación de servicio de directorio en una red de ordenadores. Es el componente que permite la validación de usuarios dentro de una red corporativa.

Dispositivo lógico: dispositivo que permite utilizar un circuito o un proyecto para muchas otras funciones con el simple cambio del software que incorpora.

Equipo: medio físico proporcionado a una persona para el correcto desempeño de sus tareas.

Estandarizado: redacción y aprobación de normas que se establecen para garantizar el acoplamiento de elementos construidos independientemente, así como garantizar el repuesto en caso de ser necesario, garantizar la calidad de los elementos fabricados, la seguridad de funcionamiento y trabajar con responsabilidad social.

FTP: siglas en inglés de *File Transfer Protocol*, 'Protocolo de Transferencia de Archivos', es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (*Transmission Control Protocol*), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Entidad de noticias: medio de comunicación dentro del sistema en el cual los usuarios leen y envían mensajes textuales a distintos tablones distribuidos entre servidores con la posibilidad de enviar y contestar a los mensajes.

Hacker: o pirata informático, es una persona que busca realizar entradas remotas no autorizadas por medio de redes de comunicación.

Hardware: todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Identificador de usuario: código alfanumérico único dentro de una red que identifica de forma unívoca a una persona o usuario de la misma.

Información: conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Macro: serie de instrucciones que se almacenan para que se puedan ejecutar de manera secuencial mediante una sola llamada u orden de ejecución. Dicho de otra manera, una macroinstrucción es una instrucción compleja, formada por otras instrucciones más sencillas.

Medio tecnológico: medio que se vale de la tecnología para cumplir con su propósito. Los recursos tecnológicos pueden ser tangibles (como una computadora, una impresora u otra máquina) o intangibles (un sistema, una aplicación virtual).

Módem: dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portador. Dispositivo físico que ayuda a la transmisión de directa de las señales electrónicas inteligibles, a largas distancias.

Monitorización de redes y sistemas: uso de un sistema que constantemente revisa una red de ordenadores buscando componentes lentos o fallidos y luego notifica al administrador de esa red en caso de cortes. Es un subconjunto de las funciones involucradas en la gestión de redes.

Nivel de privilegios: capacidad para realizar tareas dentro de una red o aplicación informática.

Password (contraseña): forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Plataforma de correo electrónico: instalación que permite disponer de un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos) mediante sistemas de comunicación electrónicos.

Recurso informático y telemático: todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento y la optimización del trabajo con ordenadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

Red: interconexión de uno o varios ordenadores y periféricos.

Registro o archivo LOG: registro de cambios dentro de una base de datos; fichero donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

Salvapantallas: programa informático diseñado para conservar la calidad de imagen del monitor y para proteger la pantalla dejando imágenes en movimiento cuando el ordenador no se está usando.

Secuencia de caracteres: secuencia ordenada de longitud arbitraria (aunque finita) de elementos que pertenecen a un cierto lenguaje formal o alfabeto.

Sistema operativo: programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

Sistema o algoritmo de cifrado: técnicas aplicadas a la ciencia, que alteran las representaciones lingüísticas de mensajes.

Sistema: conjunto de partes interrelacionadas, hardware, software y de recurso humano que permite almacenar y procesar información.

Software: equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Soporte informático: recurso tecnológico que permite la disponibilidad de una información o la obtención de la misma.

Terminal: dispositivo electrónico o electromecánico de hardware usado para introducir o mostrar datos de un ordenador o de un sistema de computación.

URL: siglas en inglés para el concepto *Uniform Resource Locator*, es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones digitales, etc.

Usuario: código alfanumérico que identifica un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso.

Virus informático: programa que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

4 DIRECTRICES

Todos los Sujetos Obligados tienen la obligación de preservar los activos de la entidad, incluyendo los sistemas, equipos e información. En este sentido, queda terminantemente prohibida la desconexión o traslado de cualquier equipo de su ubicación original sin la debida autorización.

En atención a lo mencionado en el párrafo anterior, los activos de la entidad deberán ser utilizados para propósitos relacionados exclusivamente con el COE. De igual forma, se encuentra estrictamente prohibido cualquier uso de los recursos o instalaciones de la entidad con fines ilegales y/o lucrativos, así como comerciales o profesionales distintos a los permitidos.

El usuario está obligado a utilizar la red de la entidad y sus datos e información sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la entidad o de terceros, o que puedan atentar contra la moral o las normas de ética de las redes telemáticas.

Por último, todos los Sujetos Obligados de la entidad deberán verificar que el material y la documentación de trabajo contenida en los medios tecnológicos puestos a su disposición, se encuentran debidamente guardados, y con las medidas de protección correspondientes, antes del abandono de su lugar de trabajo cada día. En este sentido, se responsabilizarán de que su estación de trabajo (por ejemplo, PC de sobremesa y /o portátiles) queda debidamente apagada o bloqueada, impidiendo cualquier acción no deseada por parte de terceros ajenos a la entidad.

Los usuarios deben notificar al Departamento de IT, a través de la dirección de correo electrónico dirtic@coe.es, cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos: pérdida de listados y/o medios de almacenamiento, sospechas de uso de su acceso autorizado (identificación de usuario y password) por terceros, recuperaciones de datos, etc.

Cuando existan indicios de uso con fines ilícitos o abusivos por parte de un Sujeto Obligado, la entidad realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoría en el ordenador del Sujeto Obligado o en los sistemas que ofrecen el servicio.

Por otro lado, el Sujeto Obligado no dejará apuntado ningún PIN o identificador de acceso en ningún lugar de fácil acceso a terceras personas.

4.1 USO DE LOS SISTEMAS

El sistema informático, la red y los terminales de la entidad empleados por cada usuario son propiedad de la misma. En este sentido, la entidad establecerá las medidas técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información de conformidad con lo dispuesto en la legislación vigente. En relación con esto, la entidad garantizará el derecho a la intimidad personal y la confidencialidad de las comunicaciones, salvo en los supuestos específicos que se prevén en la presente Política.

Todos los activos de la entidad a que hace referencia el párrafo anterior deberán ser utilizados para propósitos relacionados con el negocio de la entidad. Si en contravención con lo indicado, algún usuario realiza un uso personal de los mismos, lo hará sin ninguna expectativa de privacidad, quedando siempre a salvo la posibilidad de la empresa de realizar una auditoría de los equipos.

En este sentido, todos los Sujetos Obligados con acceso a los recursos deberán cumplir las Normas existentes sobre el uso personal de los mismos.

Con respecto al mantenimiento de la seguridad y de la red de la entidad, el personal autorizado podrá supervisar el equipo, sistemas y tráfico de la red en cualquier momento. En este sentido, la entidad se reserva el derecho de monitorizar las redes y sistemas de forma periódica.

Por su parte, ningún Sujeto Obligado podrá desactivar, bajo ninguna circunstancia, los sistemas de seguridad de su equipo ni incorporar otros, sin consultarlo previamente con el responsable de sistemas.

Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y password) está siendo utilizado por otra persona, deberá proceder a su cambio y contactar con el Responsable de Seguridad de IT para notificar la incidencia. Asimismo, los usuarios no deben utilizar ningún acceso autorizado de otro usuario.

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el Departamento de IT.

A continuación, se detallan las obligaciones de los usuarios en relación con los sistemas:

- Emplear software homologado y licenciado por el personal encargado de esta tarea dentro de la entidad. Está prohibido introducir voluntariamente programas, virus, macros, o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en las estaciones de trabajo (PC o portátil).
- Comunicar cualquier anomalía por mal funcionamiento (hardware, software, virus informáticos, etc.), al área encargada del soporte de los sistemas de la entidad, poniéndose en contacto para ello con el Centro de Ayuda al Usuario de la Entidad a través de la herramienta habilitada a tal efecto (http://servicedesk.coe.com), a través del teléfono 913815500, extensión 2190, o a través del correo electrónico support@conpaas.org.

- Habilitar las medidas de seguridad necesarias para garantizar la autoprotección de su equipo y la seguridad en su entorno de trabajo.
- Utilizar los programas anti-virus de la entidad (y sus actualizaciones), para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos. En su caso, los equipos propiedad particular del Sujeto Obligado que se empleen en el ámbito laboral de la entidad deberán poder incorporar un antivirus actualizado, así como adoptar las medidas de seguridad que el Departamento de IT determine.
- Apagar de forma ordenada la estación de trabajo al finalizar la jornada laboral. En ningún caso ésta se dejará encendida, excepto en los casos en que sea estrictamente necesario, y siempre previa autorización del Responsable de Seguridad de IT
- Bloquear la estación de trabajo en el caso de ausentarse del mismo.

Por otra parte, quedan expresamente prohibidas las siguientes actividades por parte del personal de la entidad:

- Instalar software no autorizado o no licenciado por la entidad. Los usuarios utilizarán únicamente las versiones de software facilitadas por la entidad, o cualquiera de sus empresas componentes, o cualquier otro proveedor debidamente autorizado y siguiendo sus normas de utilización. Los usuarios no deben instalar copias ilegales de cualquier programa en los puestos PC o portátiles, incluidos los estandarizados.
- Obstaculizar intencionadamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la entidad, así como realizar acciones que dañen, interrumpan o generen errores en sus sistemas.
- Destruir, alterar, inutilizar o dañar de cualquier forma los ordenadores y equipos asociados, los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.
- Introducir voluntariamente programas, virus, Macros, Applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad, o de terceros.
- Conectar a ninguno de los puestos PC o portátil ningún tipo de equipo de comunicaciones (p.e. un módem) que posibilite la conexión por un medio diferente al establecido por la entidad.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Borrar o desinstalar cualquiera de los programas instalados legalmente, así como cualquier fichero que impida o dificulte su normal funcionamiento.

4.2 IDENTIFICADORES DE USUARIO Y CLASES DE ACCESO

Las contraseñas empleadas en los sistemas y equipos de la entidad deberán ser necesariamente personales, secretas e intransferibles. Las contraseñas iniciales o reiniciadas de los usuarios serán siempre diferentes y aleatorias (procurándose que no sean parecidas al identificador, o generadas por algún algoritmo fácilmente adivinable), no utilizándose la misma contraseña por

defecto ni en el alta ni en el reinicio de las mismas. En este sentido, se forzará a los usuarios a cambiar estas contraseñas iniciales o reiniciadas en el primer acceso o uso de las mismas.

En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

En ningún caso, los Sujetos Obligados deberán comunicar a otra persona su identificador de usuario o su clave de acceso al sistema, con el fin de garantizar la confidencialidad e integridad de la misma. En este sentido, y en el supuesto de que un usuario sospeche que otra persona conoce sus datos de identificación y acceso a los sistemas deberá ponerlo inmediatamente en conocimiento del Departamento de IT, con el fin de que le sea asignada una nueva clave.

El usuario, con el objetivo de mejorar la comunicación en la entidad, acepta la publicación de su fotografía en aquellas plataformas que sirvan para una mejor identificación y comunicación tales como el directorio activo o la plataforma de correo.

Para aquellas situaciones que, por tareas de mantenimiento de los equipos, y como excepción a la norma general, el usuario deba proceder a dar acceso a sus equipos, e incluso llegar a tener que ceder la contraseña, el Sujeto Obligado deberá proceder al cambio de la misma de forma inmediata, una vez finalizadas las tareas de mantenimiento que así lo hayan requerido.

Las siguientes actividades se encuentran expresamente prohibidas:

- Compartir o facilitar el identificador de usuario y la clave de acceso (password) facilitados con otra persona física o jurídica, incluido el personal de la propia entidad.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

A la hora de crear contraseñas fuertes y efectivas deberemos tener en cuenta los métodos empleados para romperlas, por lo que, a continuación se detallan algunas acciones que deberán tenerse en cuenta en la elección de una nueva contraseña:

a) No usar palabras del diccionario, ni nombres propios o palabras extranjeras:

Las herramientas para romper contraseñas son muy efectivas procesando grandes cantidades de letras y combinaciones de números. De esta forma, también deberemos evitar utilizar palabras del diccionario seguidas de números o palabras convencionales escritas al revés. Lo que para las personas puede ser difícil de adivinar puede ser muy sencillo para estos programas de fuerza bruta.

b) No emplear información personal:

Una costumbre habitual con el objetivo de facilitar el recuerdo de contraseñas es la inclusión de información personal en las mismas.

Una de las cosas frustrantes de las contraseñas es que deben de ser fáciles de recordar por los usuarios. Naturalmente esto lleva a muchos usuarios a incluir información personal en sus contraseñas.

Para los hackers, obtener información personal sobre próximos objetivos de sus ataques puede ser fácil. Por lo tanto, las contraseñas nunca deberán incluir nada relacionado con datos de carácter personal como fechas de nacimiento, nombres de familiares, etc.

c) Longitud, anchura y profundidad:

Para que una contraseña sea considerada fuerte y efectiva se requiere de un determinado grado de complejidad. En este sentido, existen tres factores que deberán tenerse en cuenta para llegar a desarrollar este grado de complejidad, en concreto, su longitud, anchura y profundidad.

- *Longitud*: cuanto más larga es una contraseña, más difícil es de romper. Las contraseñas tendrán un mínimo de 8 caracteres. Son aceptables contraseñas más largas, siempre que el sistema lo permita, y el usuario no tenga dificultad en recordarlas.
- *Anchura*: las contraseñas cumplirán al menos uno de los siguientes requisitos, en cuanto a su anchura:
  - contendrán, simultáneamente, un carácter no alfanumérico, una letra y un número.
  - no comenzarán por el identificador del usuario.
  - no serán igual que el identificador del usuario, escrito al revés.
  - no serán adivinables con técnicas basadas en diccionario y reglas, por lo que no podrán utilizarse palabras que estén relacionadas con el usuario (domicilio, fecha nacimiento, DNI, etc.).

d) Protección Adicional:

Existen ciertas prácticas que los usuarios deberán seguir para que sus contraseñas sean lo más seguras posible. Los usuarios deben evitar utilizar la misma contraseña en diferentes cuentas, esto crea un único punto de fallo lo que significa que si un intruso accediese a una sola de sus cuentas ya tendría acceso a todas las demás.

En ningún caso, se anotarán las contraseñas en papeles u otros medios que faciliten su acceso por terceros.

e) Cambio de contraseñas:

Las contraseñas se deberán cambiar obligatoriamente cada 75 días.

Como norma general, para obtener el acceso a los sistemas de información es necesario disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que se deben observar las siguientes normas de actuación:

- Los usuarios son responsables de toda actividad relacionada con el uso de su identificador. Por tanto, no deben revelar bajo ningún concepto su acceso autorizado (identificador y contraseña), evitando teclear contraseñas en presencia de terceros.

- Los usuarios no deben mantener la contraseña por escrito a la vista, ni al alcance de terceros.
- El usuario debe utilizar una contraseña teniendo en cuenta las indicaciones contenidas en la presente Política.
- En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario deberá cambiar su contraseña como mínimo una vez cada 75 días.

4.3 USO DEL CORREO ELECTRÓNICO

Los sistemas informáticos, la red y los terminales o estaciones de trabajo utilizados por cada Sujeto Obligado son herramientas para el correcto desarrollo de la actividad profesional y son propiedad de la entidad.

Debe entenderse por correo electrónico los mensajes que se envían tanto a direcciones pertenecientes a la entidad, como a direcciones ajenas a la misma.

Con carácter general, los Sujetos Obligados de la entidad no podrán utilizar el correo electrónico, la Red de la entidad, ni el acceso a Internet para fines particulares o personales. En todo caso, para temas personales, se recomienda la utilización de un correo privado. De conformidad con lo expuesto en el apartado 4.1 en relación con el uso de los sistemas, el uso del correo electrónico se llevará a cabo sin ninguna expectativa de privacidad por parte del Sujeto Obligado, quedando siempre a salvo la posibilidad de la empresa de realizar una auditoría de los equipos.

Los Sujetos Obligados podrán utilizar el correo electrónico, la Red de la entidad, y el acceso a Internet con libertad, en el sentido más amplio posible, para el desempeño de las actividades de su puesto de trabajo. Siempre que un Sujeto Obligado de la entidad precise realizar un uso de estos medios que exceda el habitual, un envío masivo o de especial complejidad, etc., empleará los cauces adecuados, de acuerdo con su superior jerárquico o funcional inmediato, para no causar daños en el desarrollo normal de las comunicaciones o en el funcionamiento de la Red de la entidad.

Debe tenerse en cuenta que los mensajes de correo electrónico pueden ser tratados como comunicaciones públicas, por lo que debe seleccionarse cuidadosamente la información enviada por esta vía.

Los correos electrónicos que se crean en el curso normal de los negocios constituyen documentos oficiales de la entidad y podrían ser solicitados por la misma como evidencia de políticas, acciones, decisiones o transacciones oficiales.

Cuando existan indicios de uso con fines ilícitos o abusivos del correo electrónico, o de la comisión de cualquier otra irregularidad por parte de un Sujeto Obligado la entidad se reserva el derecho de revisar, los mensajes de correo electrónico enviados, recibidos o creados con la cuenta de correo electrónico de la entidad y los archivos LOG del servidor. Esta revisión se

efectuará en horario laboral, según procedimiento legal vigente, y en presencia de algún representante legal de los trabajadores, o compañero, en caso de que no haya responsable legal de los trabajadores, si el Sujeto Obligado lo desea. Esta revisión se realizará con respeto a la dignidad e intimidad del Sujeto Obligado, y con el fin de comprobar el cumplimiento de esta Política y de prevenir actividades que puedan afectar a la entidad o hacerla incurrir en responsabilidad.

Cualquier fichero introducido en la red de la entidad o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas, deberá cumplir los requisitos establecidos en esta Política y, en especial, las referidas a propiedad intelectual e industrial, así como al control de virus.

Cualquier mensaje enviado desde una dirección de correo electrónico de un Sujeto Obligado a un grupo de noticias deberá contener una cláusula (ver anexo I, incluido al final de la presente Política) en la que se establezca que las opiniones expresadas son únicamente opiniones personales, y no necesariamente las opiniones de la entidad, con la excepción de aquellos casos en los que el buzón de correo electrónico forme parte de las actividades propias de la entidad. Todos los Sujetos Obligados deberán ser precavidos con la recepción de archivos adjuntos de remitentes desconocidos.

Las siguientes actividades se encuentran expresamente prohibidas, tanto en relación con el uso de cuentas profesionales como personales otorgadas por la entidad:

- Falsificar mensajes de correo electrónico.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin su consentimiento, con el fin de vulnerar su intimidad, bien apoderándose de los mismos o bien interceptando sus comunicaciones o utilizando artificios técnicos de escucha, grabación o reproducción del sonido, la imagen o cualquier otra señal de comunicación.
- Enviar o reenviar indebidamente mensajes en cadena o de tipo piramidal.
- La utilización de la red para juegos de azar, sorteos, subastas, descarga de vídeo, audio u otros materiales no relacionados con la actividad profesional.
- Enviar información sensible de la entidad a personas no autorizadas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario (denominados comúnmente como Spam).
- Abrir archivos de fuentes con dudosa procedencia sin consulta previa al Responsable de Seguridad de IT.
- Envío de mensajes o imágenes de material ilegal, ofensivo, difamatorio, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., o de aquellos que promuevan el acoso sexual.
- Enviar mensajes con anexos de gran tamaño (archivos adjuntos con un volumen total mayor de 15 Megas) ni realizar cualquier tipo de envío sin relación alguna con el desempeño profesional, que interfiera las comunicaciones del resto de Sujetos Obligados o perturbe el normal funcionamiento de la red de la entidad.

El incumplimiento de estas normas determinará la utilización por la entidad de las restricciones que considere oportuno en la utilización de estos medios y la aplicación del régimen disciplinario, que en su caso proceda.

4.4 ACCESO A INTERNET

La utilización por parte de los Sujetos Obligados de los sistemas informáticos de la entidad para acceder a redes públicas como Internet, se limitará a aquellos aspectos directamente relacionados con la actividad de la entidad y las responsabilidades propias del puesto de trabajo del usuario, así como un uso para fines no profesionales dentro de las páginas permitidas por la entidad.

En este sentido, el acceso a páginas web (www), grupos de noticias (Newsgroups), redes sociales, y otras fuentes de información como FTP, etc. se limita a aquellos que contengan información relacionada con los cometidos del puesto de trabajo del usuario, y aquellos supuestos considerados estrictamente necesarios.

La entidad se reserva el derecho a bloquear dentro de sus tareas habituales cualquier dirección web o URL que considere oportuno, con el fin de preservar la seguridad de la red interna de la empresa y del cumplimiento de las normativas legales vigentes.

El acceso a debates en tiempo real (Chat / IRC), dado que facilita la instalación de utilidades que permiten posibles accesos no autorizados al sistema, queda terminantemente prohibido, salvo en aquellos supuestos en que esté relacionado con los cometidos del puesto de trabajo del trabajador.

Cualquier fichero introducido en la red de la entidad o en el terminal del usuario desde Internet deberá cumplir los requisitos establecidos en esta Política y, en especial, las referidas a propiedad intelectual e industrial y a control de virus. En este sentido, se prohíbe la descarga de ficheros sin autorización y verificación de calidad por el Responsable de Seguridad de IT.

La entidad podrá comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red de la entidad.

4.5 EMPLEO DEL TELÉFONO Y EL FAX

Con carácter general, el empleo del teléfono y fax, facilitados por la entidad a su personal se limitará exclusivamente para fines profesionales relacionados con la actividad de la entidad.

La entidad podrá comprobar, de forma aleatoria y sin previo aviso, la utilización por parte del personal de estos medios, siempre que se detecte de un uso irracional de los mismos.

En este sentido, se prohíbe el empleo con fines personales del teléfono para llamadas al extranjero, o a números de teléfonos con finalidades lucrativas, ilegales o inmorales.

4.6 PROPIEDAD INTELECTUAL E INDUSTRIAL

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por los derechos de propiedad intelectual o industrial de la entidad.

4.7 COMUNICACIÓN DE INCIDENCIAS Y VULNERABILIDADES

Todo el personal de la entidad está obligado a comunicar al Responsable de Seguridad de IT cualquier incidencia que se produzca en los sistemas de información a los que tenga acceso. En este mismo sentido, el personal deberá comunicar igualmente cualquier vulnerabilidad detectada o incidencia producida en cualquier medio tecnológico que se use o al cual se tenga acceso. Dicha comunicación deberá realizarse a la mayor brevedad desde el momento en que se produzca o se tenga conocimiento de dicha incidencia o vulnerabilidad. Para ello, deben dirigirse a la dirección de correo electrónico dirtic@coe.es, o comunicarlo a través del Centro de Ayuda al Usuario de la Entidad a través de la herramienta habilitada a tal efecto (http://servicedesk.coe.com), a través del teléfono 913815500, extensión 2190, o a través del correo electrónico support@conpaas.org.

Toda investigación de incidentes, así como la manipulación de la información que se origine, en cualquier tipo de soporte, será realizada por personal autorizado y con conocimientos técnicos relevantes.

4.8 EMPLEO DE DISPOSITIVOS PERSONALES

Los Sujetos Obligados de la entidad deberán asegurar el bloqueo por inactividad de cualquier dispositivo privado sobre el cual procedan a la configuración de su correo profesional, previniendo cualquier intrusión no deseada en caso de pérdida o extravío del mismo.

Se trata de proteger la información que se encuentra almacenada en las unidades compartidas de la entidad. En este sentido, para el caso de dispositivos personales que accedan al correo electrónico profesional, será también de aplicación todo lo establecido en el presente documento.

4.9 OBLIGACIONES RELATIVAS A LA SALVAGUARDA DE INFORMACIÓN

La información se ha convertido en un activo de gran importancia, por lo que las medidas de seguridad que se exponen en el apartado, en relación con la salvaguarda de información, tratan de evitar la pérdida, robo o empleo indebido de aquella información vital mediante medios tecnológicos.

En el presente apartado se identifican las acciones que los Sujetos Obligados realizarán en el caso de que se ausenten de su puesto de trabajo.

Información almacenada en disquetes, CD-ROM, cartuchos, cintas de video o cualquier otro soporte magnético:

La información que se encuentre en manos de su propietario, o de cualquier Sujeto Obligado con acceso a la misma por razón de su trabajo, se guardará en lugar seguro. En concreto, se guardará necesariamente bajo llave en cajones, armarios, etc.

Esta medida lleva aparejada otras, tales como:

- NO se dejará la llave que da acceso a la información a la vista (encima de la mesa, en el bote de los bolígrafos, en un cajón abierto, etc.).
- NO se dará acceso a la llave a nadie.

En el supuesto de pérdida o robo, o en el caso de que se tuviera sospecha de que la llave pudiera haber quedado comprometida (por ejemplo, si creemos que alguien ha podido realizar una copia o tener acceso a la llave), el Sujeto Obligado o colaborador solicitará el cambio de la cerradura del cajón o armario en el que se encuentre la información que se trata de proteger.

Información almacenada en un PC o portátil:

En el caso de que el Sujeto Obligado o colaborador se ausente de su puesto de trabajo, deberá proteger el acceso al disco duro de su PC o portátil mediante la activación de un salvapantallas protegido por contraseña. Dicha protección la activará el Sujeto Obligado manualmente (cada vez que se ausente del puesto de trabajo) y automáticamente, configurando y activando la protección en el Panel de Control/Pantalla/Protector de Pantalla, para aquellos supuestos en que, por cualquier motivo, no se hubiera bloqueado la sesión manualmente. La configuración automática permite elegir el tiempo transcurrido el cual se produce el bloqueo automático. En dicha casilla, el Sujeto Obligado seleccionará “15 minutos”.

Asimismo, al finalizar la jornada de trabajo, el Sujeto Obligado apagará el PC o Portátil, salvo en caso de necesidad justificada, en cuyo caso bloqueará la estación de trabajo con usuario y contraseña. Para sistemas que no soporten este tipo de bloqueo se empleará un salvapantallas protegido por contraseña y, si esto tampoco es posible, se apagará al menos el monitor de la estación de trabajo.

Es responsabilidad del usuario la realización de las correspondientes copias de seguridad de sus equipos de trabajo, para lo cual la entidad le facilitará los medios adecuados para su ejecución, indicándole en base al medio elegido la forma de realización de dichas copias.

Una vez que un Sujeto Obligado sea baja en la entidad, los datos almacenados en los equipos de trabajo cedidos a dicho Sujeto Obligado podrán ser accedidos por la entidad con fines profesionales, a excepción de la carpeta marcada con el nombre “Personal”, que será eliminada por el Departamento de IT, en caso de que no haya sido eliminada antes por el usuario en cuestión.

5 FORMACIÓN Y DIFUSIÓN

La presente Política se incluye entre las materias de formación obligatoria para todos los Sujetos Obligados por la misma, como parte de la formación en materia de Cumplimiento.

Se utilizarán en todo caso los siguientes canales para difundir la presente Política, en los idiomas apropiados:

a) La Intranet.
b) El Manual de Bienvenida, que se entrega a todas las nuevas incorporaciones en la plantilla del COE, el cual deberá adjuntarse la presente Política en los casos en los que se considere apropiado.

6 CONSECUENCIAS DEL INCUMPLIMIENTO

Los incumplimientos de la presente Política podrán dar lugar a la aplicación de medidas disciplinarias laborales de conformidad con lo previsto en las normas internas del COE sobre sanciones y medidas disciplinarias, concretamente la Norma Corporativa de Sistema Disciplinario.

7 APROBACIÓN, ENTRADA EN VIGOR Y REVISIÓN DE LA PRESENTE POLÍTICA

El Comité Ejecutivo del COE aprobó la presente Política en su reunión del 18 de junio de 2019, momento en el cual entró en vigor con efectos vinculantes para todos sus destinatarios.

Sin perjuicio de lo anterior, la presente Política será objeto de revisión y, en su caso, actualización, periódica.

En este sentido, el Órgano de Cumplimiento deberá elaborar un Informe Anual sobre la aplicación de la presente Política, en el que valorará si el mismo puede ser susceptible de mejora. Dicho informe será sometido al Comité Ejecutivo.

8 DOCUMENTOS RELACIONADOS

- PL003: POLÍTICA DE CUMPLIMIENTO