NORMATIVA INTERNA DE PROTECCIÓN DE DATOS PARA EL PERSONAL, VOLUNTARIOS Y COLABORADORES DE LA CRUZ ROJA ESPAÑOLA.

Con el objeto de dar debido cumplimiento a lo establecido en la Sección II (art. 32, 33 y 34) del Reglamento (UE) 2016/679, la institución Cruz Roja Española impone a su personal, voluntarios y colaboradores, en adelante "usuarios", el cumplimiento de las siguientes obligaciones, las cuales deberán ser conocidas, aceptadas y respetadas por todos ellos.

1. PROTECCIÓN DE DATOS: INFORMACIÓN Y AUTORIZACIÓN PREVIA [subir]

Todo usuario que, en el desarrollo de su trabajo, recabe datos de carácter personal de clientes, proveedores, otros empleados o terceros en general, para su incorporación a un fichero automatizado o papel, deberá informar al responsable de seguridad LOPD, al objeto de recabar su autorización y las normas aplicables para la creación, declaración y mantenimiento del fichero, a las que deberá ajustarse en todo caso.

1.1. Actos prohibidos:

a. Crear ficheros de datos personales sin la autorización del responsable, en cumplimiento de la Resolución de la Presidencia Nº 1/2005, De 5 De Mayo De 2005, Ordenadora De Los Ficheros de la Institución que contengan Datos de Carácter Personal, en vigor actualmente.

b. Cruzar información relativa a datos de diferentes ficheros o servicios, con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del responsable de seguridad.

1.1.3 Alterar la red de comunicaciones corporativa (Red IP alquilada a Telefónica) de Cruz Roja Española.

c. Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de protección de Datos.

d. Sacar soportes y ordenadores personales fuera de los locales de la organización sin la previa autorización del Secretario General o del Director del Departamento de Sistemas de Información.

2. IDENTIFICACIÓN DE USUARIOS Y CLAVES DE ACCESO [subir]

2.1. Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso, deberá ponerlo en conocimiento del responsable del sistema, con el fin de que éste le asigne una nueva clave. Ante una baja o ausencia temporal del usuario, el responsable del departamento podrá solicitar al responsable del sistema la cesión de clave o datos a la persona por él designada.

2.2. El usuario está obligado a utilizar la red corporativa y la intranet de la institución Cruz Roja Española y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la institución o de terceros, o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

2.3. El usuario esta obligados Introducir contraseña de más de 8 caracteres de longitud.

2.4. La contraseña de acceso caducará a los 90 días, debiendo ser modificada en el momento de realizar el primer acceso. Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, mascotas etc., y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.

2.5 Están expresamente prohibidas las siguientes actividades:

a) Compartir o facilitar el identificador de usuario y la clave de acceso facilitada por la institución Cruz Roja Española, a otra persona física o jurídica, incluido el personal de la propia institución. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.

b) Intentar distorsionar o falsear los registros LOG del sistema.

c) Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la institución Cruz Roja Española.

d) Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la institución Cruz Roja Española, de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).

e) Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

f) Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario (Spam).

g) Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).

h) Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la institución Cruz Roja Española y de terceros.

i) Intentar aumentar el nivel de privilegios de un usuario en el sistema.

j) 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. El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

k) Introducir, descargar de Internet, reproducir, utilizar, instalar o distribuir programas informáticos no autorizados expresamente por la institución Cruz Roja Española cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello. Por lo que todas las aplicaciones necesarias para el desempeño de la actividad laboral serán instaladas previa autorización del Responsable de sistemas de información en cada oficina o asamblea.

l) Instalar copias ilegales de cualquier programa, incluidos los estandarizados.

m) Borrar cualquiera de los programas instalados legalmente.

n) Utilizar los recursos telemáticos de la institución Cruz Roja Española incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

ñ) Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la institución Cruz Roja Española, en la red corporativa de la Instituci&oaute;n.

o) Enviar o reenviar mensajes en cadena o de tipo piramidal.

3. CONFIDENCIALIDAD DE LA INFORMACIÓN: [subir]

3.1. Queda prohibido enviar información confidencial de la institución Cruz Roja Española al exterior, mediante soportes materiales, o a través de cualquier medio de

comunicación, incluyendo la simple visualización o acceso.

3.2. Los usuarios de los sistemas de información de la institución Cruz Roja Española deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación con la institución Cruz Roja Española, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato o relación.

3.3. Ningún usuario deberá poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la institución Cruz Roja Española, tanto ahora como en el futuro.

3.4. En el caso de que, por motivos directamente relacionados con el puesto o actividad, el usuario entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, titularidad o copia cobre la referida información. Asimismo, el usuario deberá devolver dichos materiales a la institución Cruz Roja Española, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización del contrato o relación. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la institución Cruz Roja Española, no supondrá, en ningún caso, una modificación de esta cláusula.

3.5. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el código Penal y recogido en el Plan de Riesgos Penales, en relación a los artículos: - Delitos contra la intimidad y allanamiento informático art. 197.
- Daños Informáticos, destrucción, borrado, robo de información, sustitución de un sistema informático.
- Hacking art. 264 y 264 bis.
- Uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular art. 256.

En función de la gravedad de los hechos, la institución Cruz Roja Española podrá iniciar las acciones legales que correspondan contra la persona o personas presuntamente responsables de los mismos, incluyendo las consecuencias disciplinarias internas y cuantas otras estime pertinentes.

3.6. El usuario que tenga acceso a los documento para el desarrollo de su actividad o tratamiento, está en la obligación de custodia de los mismos, así como en la de informar a su responsable de las incidencias que puedan ocurrir durante su tratamiento.

3.7. Activar el salva pantalla para periodos de inactividad mayores de 10 minutos.

3.8. En el caso que sea necesario la duplicación de los documentos, impresión de los mismos o traslado fuera de la institución o centros de la Cruz Roja Española, el usuario está en la obligación de reflejar en un documento de Entrada/Salida los movimientos de los contenidos duplicados o documento originales; previa autorización del Responsable.

3.9. Todos los documentos que sean impresos y que contengan datos de carácter personal, así como su retirada de las bandejas de las impresoras o fotocopiadoras, es responsabilidad de la persona que realiza dichos procesos. La pérdida o extravío de estos documentos pueden acarrear medidas de carácter disciplinario o administrativo, según correspondan.

3.10. Toda documentación a la que tenga acceso, que contenga datos de carácter personal y que no sea necesaria su conservación, está en la obligación de destruirla, de forma tal que imposibilite la obtención de dichos datos. Los documentos (folios) que contengan datos de carácter personal no pueden ser reutilizados, a menos que se garantice su custodia y posterior destrucción una vez no sean necesarios.

3.11. Las mesas/despachos de los profesionales/trabajadores, personal de administración, voluntarios y colaboradores, que contengan carpetas o documentos con datos de carácter personal, deben estar dotados de los mecanismos de control necesarios que permitan su recogida, almacenamiento y custodia, una vez que abandonen el puesto o concluya su jornada (archivadores con llave).

3.12. Velar constantemente por la privacidad de los datos contenidos en los documentos, tomando las medidas necesarias para evitar que puedan ser leídos o vistos por persona ajena no autorizada, cumpliendo con el deber de secreto.

Los responsables de los locales o archivos donde se encuentren los documentos con datos de carácter personal, deben asegurarse que éstos permanecen bajo llave u otro mecanismo que imposibilite que personas no autorizadas puedan tener acceso a los mismos.

3.13.Los documentos en papel deben estar colocados de forma ordenada y en lugares adecuados para su conservación, localización y acceso, permitiendo garantizar, de forma eficiente, su localización, con el objeto de cumplir los plazos en el ejercicio de los Derechos de los Afectados.

3.14. La persona que se encuentra a cargo de documentos que se encuentren en proceso de revisión, modificación o tramitación, ya sea previo o posterior a su archivo, deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

4. CORREO ELECTRÓNICO, INTERNET, DISPOSITIVOS MÓVILES Y REDES SOCIALES **[subir]**

La institución Cruz Roja Española pone en conocimiento de todos sus usuarios (empleados, voluntarios y colaboradores) que el acceso a Internet y el servicio de correo electrónico es un medio proporcionado por la institución y que estará sujeto a los controles internos previstos que garanticen su correcta explotación y el uso adecuado del servicio, por lo que se reserva el derecho de controlar y, en los casos que considere necesario, inspeccionar sus contenidos. La utilización de este medio en contra de los intereses de la institución Cruz Roja Española, originará las acciones y/o las sanciones correspondientes, según corresponda.

La navegación a través de Internet debe estar dirigida a aquellos sitios que sean necesarios para el cumplimiento de las labores propias de la institución, por lo que la institución se reserva el derecho de controlar el uso de la misma así como de establecer los mecanismos que impidan la libre navegación.

4.1 Uso del correo electrónico corporativo

1. El uso del correo electrónico queda limitado a fines estrictamente laborales y relacionados con las funciones desarrolladas por el personal de Cruz Roja. Se considerará correo electrónico, tanto el interno (circulando entre terminales de la red informática de la Cruz Roja, como el externo (dirigido o proveniente de otras redes públicas o privadas, en especial, Internet).

2. Como norma general, los empleados no están autorizados a utilizar el correo electrónico, la Red Informática o Internet para fines privados.

3. Los mensajes de correo electrónico pueden ser tratados como comunicaciones públicas, por lo que hay que seleccionar con cuidado la información que se envía por correo electrónico, y tomar las medidas adecuadas para protegerla.

4. Cruz Roja se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico enviados, recibidos o redactados utilizando la cuenta de correo electrónico de la organización, así como los archivos LOG del servidor, para comprobar que cumplen estas normativas y que no generan actividades que afecten negativamente a Cruz Roja o que impliquen su responsabilidad.

5. Cualquier correo electrónico enviado desde la dirección de un empleado, voluntario de Cruz Roja a un grupo de noticias o a un foro, debe incluir una cláusula que precise que las opiniones ahí expresadas son sólo opiniones personales, y que no tiene por qué ser la opinión de Cruz Roja, salvo en el caso en el que el correo electrónico forme parte de las actividades propias de la organización.

6. Todos los empleados deberán tener un cuidado extremo al recibir archivos adjuntos enviados de fuentes desconocidas.

7. El envío de datos personales mediante redes de telecomunicaciones, considerados de nivel alto se realiza codificando los datos o utilizando cualquier otro software/dispositivo que garantice que la información no es legible ni manipulable por un tercero.

8. Se prohíben expresamente las siguientes actividades:

   a. Falsificar mensajes de correo electrónico

   b. Envío o reenvío inadecuado de cadenas de correos electrónicos.

   c. Abrir archivos de origen dudoso sin consultar previamente a la persona responsable de sistemas.

   d. Enviar mensajes o imágenes ilegales, ofensivas, difamatorias o de carácter inapropiado, o con contenido discriminatorio en cuanto al género, edad, sexo,

discapacidad, etc., o enviar material que fomente el acoso sexual.

El incumplimiento de estas normas implicará la aplicación por parte de Cruz Roja de las restricciones que se consideren adecuadas por haber participado en las actividades anteriormente mencionadas, aplicando medidas disciplinarias cuando se estime oportuno

En caso de que haya indicios de uso abusivo o ilícito por parte de un empleado, la institución realizará las comprobaciones pertinentes y, si procede, revisará el ordenador del empleado o los sistemas que ofrecen ese servicio. Esto se llevará a cabo en horario laboral en presencia de un representante del trabajador o de su sindicato (en caso de estar afiliado) y si el empleado así lo desea, respetando la dignidad y privacidad del mismo.

4.2 Uso de Internet

Del mismo modo, el uso de Internet queda limitado a fines estrictamente laborales y relacionados con las funciones desarrolladas por el personal de Cruz Roja. Se considerará acceso a Internet, el que se realice empleando la red inalámbrica o inalámbrica que Cruz Roja pone a disposición de sus trabajadores e, incluso, el uso y empleo de las direcciones IP en las que radicase tal acceso. Se permitirá un uso personal de internet siempre que sea razonable y no afecte al desarrollo de las funciones del Empleado exigido por Cruz Roja.

a. Está expresamente prohibido el empleo de la conexión a Internet facilitada por Cruz Roja para acceder a páginas de contenidos lúdicos, descargas, obscenos, y/o chats, así como cualesquiera otros que tuvieran un carácter similar a los anteriormente descritos.

b. El uso de los sistemas informáticos Cruz Roja para acceder a redes públicas como Internet estará limitado a aquellos aspectos directamente relacionados con la actividad de Cruz Roja y con las responsabilidades del usuario derivadas de su trabajo.

c. Acceder a chats/IRC es especialmente peligroso, ya que esto facilita la instalación de herramientas que pueden permitir el acceso no autorizado al sistema. Por tanto, su uso queda prohibido, salvo en el caso de que esto esté relacionado con el trabajo del empleado.

d. El acceso a páginas web, grupos de noticias y otras fuentes de información como el FTP, etc., se limita a aquellos sitios que contengan información relacionada con la actividad de Cruz Roja o con el trabajo que desempeña el usuario así como otras que se consideren estrictamente necesarias.

e. Cruz Roja se reservan el derecho de supervisar y controlar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa

f. Cualquier archivo descargado de Internet a la red de Cruz Roja o al terminal del usuario deberá cumplir los requisitos establecidos en este reglamento y, de forma específica, los relacionados con la propiedad industrial e intelectual y el control de virus.

g. Queda prohibido descargar archivos no autorizados sin que la persona responsable del sistema, verifique la calidad de los mismos.

h. El acceso a Internet solo estará permitido utilizando software aprobado por Responsable de Seguridad. El área de sistemas aprueba y solicita el software no convencional que sea necesario para desempeñar las obligaciones laborales de un usuario. Sólo el departamento de sistemas está autorizado a instalar dicho software.

4.3 Uso del teléfono y dispositivos móviles

El uso del teléfono fijo o dispositivo móvil puesto a disposición del empleado por Cruz Roja, queda limitado a fines estrictamente laborales y relacionados con las funciones desarrolladas por el personal de Cruz Roja. Se considerará empleo del teléfono, cualquier comunicación realizada desde números de Cruz Roja, independientemente de que se efectúe o no desde el terminal que es puesto a disposición para su uso personal.

Cruz Roja podrá comprobar el empleo realizado de las líneas telefónicas cuya titularidad ostente, quedando expresamente facultada para requerir a los empleados usuarios de las mismas, para que faciliten información pertinente sobre su uso.

Los usuarios quedan enterados y consienten de forma expresa que pueda revisarse sus extractos o registros de consumo, así como que puedan efectuarse comprobaciones sobre la relación que los mismos guardan con la actividad laboral diaria.

4.4 Redes sociales

Los perfiles y páginas corporativas de Cruz Roja tienen por finalidad establecer un nuevo canal de comunicación con nuestros clientes, analizar sus necesidades y preferencias, así como anunciar los servicios, ofertas y promociones que pueden resultar atractivas para nuestros clientes.

Por todo ello, le comunicamos a todo el personal que con la finalidad establecer un único canal de comunicación y de este modo evitar crear cualquier tipo de confusión a nuestros usuarios y seguidores los empleados de las sociedades de Cruz Roja no están autorizados a:

- Utilizar el logo, marca e imagen de Cruz Roja en sus perfiles y cuentas personales en las redes sociales.

- Publicar en su perfil comentarios a título personal de cualquier índole relacionados con las sociedades de Cruz Roja, sus actividades, oferta, promociones, y/o campañas.

5. Registro de las Incidencias de seguridad:

5.1- Es obligación de todos los usuarios de la institución Cruz Roja Española comunicar al responsable del sistema cualquier incidencia que se produzca en los sistemas de información, así como en los archivos y documentos con datos de carácter personal a que tengan acceso.

5.2- Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

5.3- Dicha comunicación deberá realizarse en un plazo de tiempo no superior a una hora (1) desde el momento en que se produzca dicha incidencia, utilizando la aplicación de Registro de Incidencias o dirección de e-mail alternativo **dpo@cruzroja.es**.

Fecha de revisión Mayo 2018.