



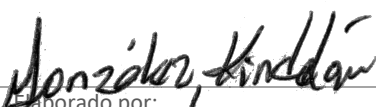


Cruz Roja Panameña

POLÍTICA DE TECNOLOGÍA DE LA INFORMACIÓN (IT)

Resumen

La presente política define las limitaciones y obligaciones de los usuarios para preservar la seguridad de la información

CRUZ ROJA PANAMEÑA

		
Elaborado por: Oficial IT – Transformación Digital	Revisado por: Directora General	Autorizado por: Presidente Nacional
Elaboración versión: 15.07.2024	Fecha de Revisión: 17.07.2024	Fecha de Autorización: 24.08.2024

Control de firmas del documento

Versión 01- 24.08.2024

Elaborado por: Kindelán González – Oficial IT

Revisado por: Larissa Rodríguez – Directora General

Autorizado por: Elías Solís – Presidente Nacional

Contenido

1. Glosario	3-4
2. Introducción.....	5
3. Objetivo.....	6
4. Ámbito de aplicación y alcance	6
5. Requisitos para la seguridad de la información.....	6
6. Prácticas obligatorias y responsabilidades del usuario	6-7
7. Uso aceptable de recursos y tecnologías de la información y las comunicaciones.....	7-8
8. Uso inaceptable de recursos y tecnologías de la información y las comunicaciones.....	8-9
9. Uso personal	9
10. Uso del correo electrónico.....	10-15
11. Seguridad	15
12. Derecho de autor, licencias y programas informáticos.....	16
13. Cumplimiento de normas y procesos.....	16
14. Sanciones	16
15. Declaración de conformidad	17
16. Anexos: Controles de clasificación de la información	17-24

Glosario

TI: Tecnología de la información y las comunicaciones, mejor conocido como IT

Activo de información: Conjunto de información identificable, almacenada en un determinado formato (electrónico, impreso) y con valor reconocido en lo que atañe a los propósitos de la organización en el cumplimiento de sus funciones institucionales.

Categorías de clasificación de la información: Categorías en función de las cuales y según criterios específicos, se define la clasificación de la información.

Confidencialidad: Característica según la cual la información no se pone a disposición de personas, entidades o procesos no autorizados, ni se les comunica.

Controles de clasificación de la información: Controles que definen el tratamiento que se dará a los activos de información, con arreglo a su clasificación.

Disponibilidad: Capacidad de un usuario para acceder a la información que necesite en una ubicación específica y en el formato adecuado.

Empleado: Este término hace referencia al personal de la Cruz Roja Panameña. Incluye a todos los miembros del personal de gestión y delegados de otras Sociedades Nacionales o del Movimiento

Información para la identificación personal: Datos que, por sí solos o en combinación con otra información, sirven para identificar, localizar o ponerse en contacto con una persona (por ejemplo, nombre, dirección de correo electrónico, fecha de nacimiento, número de pasaporte, número de seguridad social o antecedentes penales).

Integridad de la información: Protección de la información de manera que sea exacta y completa durante todo su ciclo útil.

Período de retención: Los registros de la Cruz Roja Panameña se deberán eliminar con previa autorización de Gobernanza y/o Dirección General, bajo el término aprobado.

Personal: Las expresiones personal y miembros del personal hacen referencia a los empleados de la Cruz Roja Panameña Incluye a todos los miembros del personal administrativo, los voluntarios, los pasantes, los consultores, proveedores de servicios y a todas las personas que realizan actividades en nombre de la Cruz Roja Panameña.

Política de escritorio limpio: política que exige a los miembros del personal que, al final de cada jornada y antes de salir de la oficina, guarden todos los documentos que estén a la vista.

Principio de conocimiento justificado: el acceso a la información debe estar restringido al número mínimo de personas que lo necesiten para el ejercicio de sus funciones oficiales.

Propietario del activo de información: persona o grupo de personas identificadas como responsables de velar por el carácter confidencial del activo de información. Salvo determinación En contrario, se considerará propietario del activo de información a la persona responsable de la gestión de dicha información.

Seguridad de la información: proceso por el cual se protege los datos contra todo acceso no autorizado durante su almacenamiento, tránsito o tratamiento, uso, divulgación, destrucción, modificación o alteración, bien accidental o intencional. Mediante los procesos de seguridad de la información se preserva el carácter confidencial, la integridad y la disponibilidad de la información.

Usuarios: En el presente documento, el término “usuarios” hace referencia a todos los miembros del personal de la Cruz Roja Panameña, los contratistas y los terceros proveedores que gocen de autorización para acceder, tratar o utilizar la información o los datos de la Cruz Roja Panameña.

RRHH: Departamento de Recursos Humanos.

DG: Dirección General

SDG: Subdirección General

CG: Coordinación General

PN: Presidencia Nacional

Nota: En aras de la sencillez de redacción, cabe entender que mediante el uso de denominaciones en masculino, singular o plural, en este documento se abarca a hombres y mujeres, reconociéndose que se trata apenas de un imperativo gramatical que no refleja parcialidad alguna en cuanto a género.

Introducción

La Cruz Roja Panameña confiere distintos usos y destinos a la información que recibe y procesa. La reputación de la Cruz Roja Panameña, así como la eficacia y la eficiencia de la labor que realiza, puede verse expuesta a considerable riesgo en caso de que los usuarios (es decir todos los miembros del personal, los contratistas y los terceros proveedores que gocen de autorización para acceder tratar o utilizar la información a los datos de la Cruz Roja Panameña) incumplan las no las normas y los controles adecuados en lo que atañe a la gestión de la seguridad de información.

Es responsabilidad del departamento de tecnologías de la información (TI) de la Cruz Roja Panameña preservar la seguridad y la integridad de los sistemas de información y comunicaciones de la organización. Junto con el departamento de RRHH, vela por que los usuarios conozcan el marco de seguridad de la información establecido por la Cruz Roja Panameña y las normas de la conducta que se espera de ellos en el empleo de los recursos y las tecnologías de la información y las comunicaciones. El departamento de TI también es responsable de velar por que se adopten las medidas necesarias si no se cumplen esas normas, avalado por la Dirección General.

1. Objetivos.

La presente política define las limitaciones y obligaciones de los usuarios en las siguientes actividades:

- Aplicar los controles adecuados para preservar la seguridad de la información
- Utilizar los recursos y las tecnologías de la información y las comunicaciones de manera eficaz, eficiente y coherente con los principios fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (Movimiento).

2. Ámbito de aplicación y alcance.

La presente política es aplicable a todos los usuarios. Esta política concierne a las Sociedades Nacionales, aliados, donantes, socios que hayan firmado un acuerdo con la Cruz Roja Panameña y estén sujetas al ámbito de responsabilidad en materia de seguridad de la organización, lo que incluye la observancia del código de conducta de esta.

La política será de aplicación obligatoria con respecto a los activos de información y datos en cualquier formato, a título enunciativo y no exhaustivo de documentos impresos, datos electrónicos, imágenes, conversaciones orales, equipos informáticos, equipos de comunicación en red o de datos, programas informativos, soporte lógico de procedimientos y de apoyo, y disposición de almacenamiento de datos. Se revisará cada dos años, por conducto del área IT de la Sociedad Nacional.

3. Requisitos para la seguridad de la información.

Los usuarios tienen la responsabilidad de aplicar los controles apropiados con el objetivo de mitigar los riesgos relativos a la seguridad de la información o los datos a los que tengan acceso y que traten o utilicen, así como de informar sobre todo fallo en la seguridad a las personas responsables competentes con la responsabilidad de la Cruz Roja Panameña.

4. Practicas obligatorias y responsabilidades del usuario.

El usuario deberá seguir las normativas generales que se presentan a continuación con objeto de reducir al mínimo los riesgos para la seguridad de la información.

- Los usuarios no deberán almacenar información en el disco local (C:\) ni en el escritorio del ordenador, ni en la carpeta de descargas del equipo. La salvaguarda de documentos en el escritorio del ordenador obstaculiza la flexibilidad de las tareas y retarda el acceso al sistema.

Además, genera un riesgo de pérdida de los datos, ya que el departamento de TI no establece copias de seguridad de la unidad local ni de la carpeta de descargas.

- Los usuarios deberán bloquear los ordenadores antes de dejarlos desentendidos durante periodos breves y cerrar la sesión en caso de ausencia prolongada.
- Los usuarios no deberán colocar ni descargar imágenes personales para ubicarlos en el escritorio del equipo.
- Cuando se contrate a personal temporal u ocasional se deberá determinar los sistemas y carpetas de datos a los que tendrán acceso esos usuarios para cumplir con sus obligaciones antes de solicitar al departamento de IT que se configure el acceso a la red.

5. Uso aceptable de recursos y tecnologías de la información y las comunicaciones.

El uso de los recursos de las tecnologías de la información y comunicaciones de la Cruz Roja Panameña se concede con arreglos a los principios que se exponen a continuación:

- Se podrán utilizar los recursos y las tecnologías de la información y las comunicaciones solamente con fines legítimos que tengan relación con las actividades de la Cruz Roja Panameña. Al utilizar esos recursos, los usuarios deberán respetar y promover los niveles más elevados de conducta ética y profesional, todo uso inapropiado de esos recursos dará lugar a medidas disciplinarias que podrán conllevar incluso la destitución/desvinculación del cargo.
- Los recursos y tecnologías de la información y comunicaciones se utilizarán con arreglo a los principios fundamentales del Movimiento, a la presente política y al código de conducta de la Cruz Roja Panameña.
- Los usuarios serán responsables del cuidado de los equipos de tecnologías de la información y las comunicaciones que hayan recibido (ordenadores de escritorio, portátiles, teléfonos móviles, satelitales, entre otros). La pérdida de cualquier equipo (ordenadores de escritorio, portátiles, teléfonos móviles, satelitales, entre otros) deberá comunicar cuanto antes al jefe inmediato y al departamento de TI aportando detalles sobre los datos almacenados en él.

- El empleo de los recursos de las tecnologías de la información y las comunicaciones deberá respetar todas las leyes nacionales e internacionales aplicables al fraude informático, la pornografía, el uso indebido del equipo o los recursos, el carácter confidencial de la información y cualquier delito penal conexo, así como cualquier otro requisito legal, como las obligaciones en materia de derechos de autor y concesiones de licencias.
- El empleo de los recursos y las tecnologías de la información y las comunicaciones podrá estar sujeto a supervisión por motivos de seguridad, gestión de la red u otros y a ciertas limitaciones.

6. Uso inaceptable de recursos y tecnologías de la información y las comunicaciones.

Se considerará inaceptable todo empleo de los recursos y tecnologías de la información y las comunicaciones con fines que sean ofensivos, ilegales o contrarios al código de conducta, la presente política, el reglamento interno de trabajo o las políticas de RRHH. A continuación, figuran ejemplos de actividades que son inaceptables y están prohibidas:

- El empleo de los recursos y las tecnologías de la información y las comunicaciones de la Cruz Roja Panameña de manera que no guarda consonancia con el código de conducta o de la presente política.
- La descarga, el envío de mensajes de correo electrónicos, la visita intencional a sitios web o cualquier otro tipo de acceso a material indecente, pornográfico, que incite al odio o sea censurable por cualquier motivo (a menos que sea necesario específicamente para el ejercicio de las funciones oficiales). El acceso a ese tipo de material podrá constituir una falta de conducta grave y dar lugar a la destitución/desvinculación sumaria, es decir, del usuario.
- Todo intento para superar o desactivar las medidas de seguridad, acceder a datos o modificarlos sin contar con la autorización debida.
- El empleo de recursos y las tecnologías de la información y las comunicaciones con una identidad ficticias o pertenecientes a otra persona (a menos que sea necesario para el ejercicio de las funciones oficiales, por ejemplo, para comprobar los sistemas informáticos.
- El uso o la instalación de dispositivos no normales o de programas informáticos no aceptados y autorizados. Todo uso de los sistemas de información deberá ser conforme a las obligaciones contractuales de la Cruz Roja Panameña, con inclusión de las limitaciones definidas en los programas informáticos y otros contratos de concesión de licencias.

- Los usuarios no configuraran reglas en Outlook para el reenvío de correo electrónico a sus direcciones personales ni a ninguna otra dirección ajena a la Cruz Roja Panameña. Con ello se reduce el riesgo de que el material de carácter reservado sea reenviado a sistemas de correo electrónico cuya seguridad sea inadecuada.
- El empleo de los recursos y las tecnologías de la información y las comunicaciones en contravención del derecho civil o penal. Los usuarios deben ser conscientes que esto incluye el incumplimiento de las leyes de derecho de autor, que rigen la copia, la visualización y el uso de programas informáticos y demás obras en formato digital.

7. Uso personal.

La Cruz Roja Panameña permite a los usuarios un uso personal razonable y limitado de los recursos informáticos. Corresponde exclusivamente a la Cruz Roja Panameña la responsabilidad de determinar qué uso es “razonable”, teniendo en cuenta las circunstancias pertinentes. La Cruz Roja Panameña puede imponer límites a ese uso personal, o ponerle fin, si lo considera apropiado. Los recursos y las tecnologías de la información y las comunicaciones están destinados al ejercicio de funciones oficiales.

El uso personal no interferirá con el funcionamiento de la red, no obstaculizará la labor de otros usuarios ni los distraerá en el ejercicio de sus funciones. Además, el uso personal no dará lugar a costos ni responsabilidades adicionales para la Cruz Roja Panameña. Tampoco podrá menoscabar de manera significativa la capacidad de un usuario para realizar la labor que se le ha asignado. Los siguientes son ejemplos de actividades con probabilidades de efecto adverso en la Cruz Roja Panameña (bien sea en términos de costo, capacidad de la red u otros):

- Llamadas telefónicas personales.
- Servicios con uso intensivo de datos (como la transmisión en continuo de vídeo o datos).
 - Videoconferencias con fines personales
- Juegos interactivos
- Descarga de archivos personales de gran volumen y servicios de mensajería interactiva.

Si un miembro del personal desconoce el efecto eventual del uso de tales recursos, deberá solicitar asesoramiento al personal del Departamento de TI.

Aunque la Cruz Roja Panameña permite a los usuarios emplear ocasionalmente los sistemas informáticos de la organización (dentro de un margen razonable) para almacenar archivos personales o transmitir mensajes privados, se trata de un servicio prestado por cortesía y bajo responsabilidad del propio usuario. La Cruz Roja Panameña no puede garantizar el carácter confidencial, ni es responsable de esos archivos o mensajes, y podrá limitar o poner fin a esas actividades cuando lo considere necesario.

8. Uso del correo electrónico.

Los usuarios deben ser conscientes de que, cuando envían un mensaje de correo electrónico desde una dirección “___@cruzroja.org.pa”, lo hacen en representación de la Cruz Roja Panameña. Los mensajes electrónicos pueden ser jurídicamente vinculantes para la Cruz Roja Panameña y exponer a la organización a responsabilidades jurídicas o perjuicios para su reputación. Por consiguiente, los usuarios deberán asegurarse de que observan rigurosas normas éticas. Son ejemplos de prácticas inaceptables relacionadas con el correo electrónico, entre otras:

- Responder de manera rotundamente hostil, insultante o incendiaria
 - Enviar correo basura o mensajes en cadena.
- Suplantar la identidad de otro usuario.
- Enviar mensajes ofensivos o censurables.

Los usuarios deberán aplicar controles apropiados para velar por la seguridad de la información y seguir las prácticas recomendadas en relación con el correo electrónico, como archivar, reducir al mínimo el tamaño de los archivos adjuntos y evitar **“responder a todos”** cuando no sea necesario. No se deberá guardar los mensajes y archivos personales en el sistema durante un período superior al estrictamente necesario. Los mensajes electrónicos enviados o recibidos en calidad de comunicaciones oficiales constituyen registros de la Cruz Roja Panameña y deberán conservarse durante el tiempo que sea necesario conforme a los requisitos administrativos y jurídicos de la Cruz Roja Panameña.

El sistema de correo Electrónico es propiedad de la Cruz Roja Panameña y TODAS las copias de mensajes creados, enviados, recibidos o almacenados en dicho sistema son y permanecerán como propiedad de la Cruz Roja Panameña, con el fin de comunicar temas relacionados con la Sociedad. Este correo no debe considerarse en ningún momento de uso personal sino para utilidad de la Sociedad Nacional.

La Cruz Roja Panameña se reserva el derecho de: Auditar, interceptar, acceder, monitorear, borrar o divulgar cualquier mensaje creado, recibido, enviado o almacenado en el Sistema de Correo Electrónico para el propósito de salvaguardar la imagen de la Cruz Roja Panameña.

a) Creación / eliminación de un correo electrónico

Para proceder a la creación de un correo electrónico institucional se debe recibir una solicitud de alguno de los siguientes grupos de personas:

- RRHH
- DG
- SDG
- CG

Si un usuario solicita la creación de un correo electrónico institucional, esta solicitud debe estar aprobada por alguno de los grupos antes mencionados.

El nombre de usuario de cada correo institucional se creará de la siguiente manera: nombre.apellido@cuzroja.org.pa. Para nombre y apellido repetidos dentro de la organización se colocará un número secuencial al final de apellido; de la siguiente manera: nombrerepetido.apellidorepetido1@cuzroja.org.pa.

Toda solicitud de creación de correo electrónico tiene un rango de espera como mínimo de 5 días y máximo de 2 semanas, este tiempo en calculado basado en los trabajos a realizar a la hora de creación de un correo electrónico, organización del nuevo miembro de la institución y documentación a realizar.

Es responsabilidad de cada departamento mantener todos sus documento respaldados y centralizados para evitar perdida de documentos con la salida del personal, toda verificación de datos debe ser verificada antes de la salida del personal. Es responsabilidad del departamento de RRHH notificar la fecha de salida de todo personal en el momento en que se hace de su conocimiento para que el departamento de TI proceda a revocar los accesos de correo electrónico de dicha persona. El departamento de RRHH también deberá recibir el equipo de cómputo del personal retirado y hacer entrega de este al departamento de TI para proceder a formatear y/o desechar el equipo, basado en el anexo: *Controles de clasificación de la información*.

Para personal voluntario, las acciones del departamento de RRHH serán asumidas por PN, DG, SDG, CG.

El departamento de TI no se hace responsable por la perdida, filtrado y/o robo de información ocasionado al no notificar la salida de un colaborador y/o voluntario a tiempo.

b. Acceso a correos institucionales

Cruz Roja Panameña le brindara acceso a un correo electrónico personalizado a los siguientes grupos de personas:

Grupo	Acceso (si/no)
Colaboradores de la SN	Si
Juta Directiva Nacional (JDN)	Si
Presidentes Locales y directores nacionales de organismos voluntarios.	Si
Puntos Focales	Si
Comité Central	No
Voluntarios	No

c. Medidas de seguridad

- Todo correo de La Cruz Roja Panameña debe ser manejado bajo el dominio “cruzroja.org.pa” es decir, todo correo perteneciente a Cruz Roja Panameña debe finalizar en “@cruzroja.org.pa”.
- El Sistema de Correo Electrónico debe ser utilizado solo para manejo y coordinación del propósito de la Cruz Roja Panameña. No está autorizada la utilización de este sistema para cualquier propósito diferente a éste.
- Los usuarios del sistema de correo electrónico deben abstenerse de enviar por este medio información confidencial, privada, reservada o personal, a menos que esté debidamente justificada en los lineamientos establecidos por las disposiciones legales que rigen el tratamiento de datos Personales (*Ley 81 de protección de datos personales y/o el Manual de Protección de datos en la Acción Humanitaria*) o por consentimiento libre e informado del titular de la información. (mantener constancia escrita u oral)
- Cada usuario es totalmente responsable de la utilización de su cuenta de correo electrónico, por lo cual, deberá mantener las contraseñas estrictamente secretas y mantener bloqueos de pantalla en caso de no estar en su puesto de trabajo o alejado de su equipo.

- Se prohíbe enviar correos masivos para asuntos de índole personal a las cuentas individuales o, en general, a cualesquiera otras cuentas, así como divulgar asuntos inherentes únicamente a la Sociedad Nacional.
- El envío o recepción de archivos adjuntos a los mensajes de correo electrónico está sujeto a su previa revisión por parte del antivirus que el departamento de TI considere utilizar para efecto de evitar ataques de virus u otros códigos maliciosos.
- El tamaño máximo de los mensajes enviados no debe sobrepasar los 35,840 KB, mientras que los mensajes recibidos un máximo de 36,864 por mensaje; o el tamaño que la Cruz Roja Panameña estipule de acuerdo con las necesidades, pero no más de 153,600 KB.
- Se debe tener especial cuidado en abrir y reenviar correos de dudosa procedencia, sobre todo aquellos que hagan alusión a alguna noticia sensacionalista como sucesos con celebridades, desastres naturales, etc. Usualmente son usados como medio para propagar el Phishing (suplantación de identidad).
- Evitar “responder a todos” cuando no sea necesario.
- No se debe participar en la propagación de cartas en cadenas, ni en esquemas de piramidales de índole político, religioso o temas similares, o cualesquiera otros temas que nos sea compatible con los principios fundamentales del Movimiento.
- Se prohíbe a los usuarios suscribirse a foros de discusión u otras agrupaciones ofrecidas por Internet ajenas a las funciones que desempeña en la Cruz Roja Panameña y con la utilización de la cuenta de correo de la Sociedad Nacional.
- Cualquier empleado que descubra una violación a las políticas de utilización del Sistema de Correo electrónico, estará en la obligación de señalarla a su superior o jefe de área.
- Es una falta grave facilitar y ofrecer su cuenta de correo (e-mail) a personas no autorizadas, su cuenta es personal a uso institucional e intransferible y no debe permitirse el acceso de terceros a una dirección de correo electrónico de la Sociedad Nacional.
- Toda información o contenido que sea transmitido por las cuentas de correo, son responsabilidad únicamente del dueño de la cuenta por lo que dichos contenidos no reflejan las preferencias de la Cruz Roja Panameña.

- Todo correo emitido, deberá contener un pie de página (mejor conocido como: *firma de correo electrónico*) definido por La Cruz Roja Panameña y solo podrá utilizarse el mismo (ninguno de carácter personal, ni con logos diferentes, ni artes o cualesquiera motivos que distraiga los principios fundamentales del Movimiento). Este pie de página deberá contener entre otra información: nombre y cargo del trabajador/voluntario, nombre del departamento, número de teléfono y extensión. No se debe alterar el formato de correo establecido (pie de página, formato de texto, deslinde de responsabilidad etc.)
- Cuando un colaborador y/o voluntario este de licencia, vacaciones, viajes de trabajo, deberá dejar activado el mensaje de respuesta automática al emisor del email, indicando en el mismo, el período durante el cual no estará en la oficina, la persona a la cual deberá contactar en caso de así desearlo, junto con la dirección de correo electrónico, número de teléfono y extensión de la persona que lo reemplazará durante su ausencia. Este mensaje debe ser activado tanto para emisores externos a la organización, como para emisores interno, siempre cuidando los datos compartidos en el mensaje automático para emisores externos, se prohíbe el uso de datos sensibles en este.
- La información personal recibida mediante correo debe permanecer en archivo el tiempo que sea necesario para ser requerida y deberá ser destruida o borrada una vez culmine el período de utilidad de esta.
- Los equipos informáticos o móviles o cualesquiera equipos de uso personal donde se accede a la información de la cuenta de correo de la Cruz Roja Panameña, en caso de daño del equipo o, hurto o acceso indebido será responsabilidad del empleado y/o voluntario, si se confirma su responsabilidad en el acceso indebido, estará sujeto a acciones disciplinarias de acuerdo con las normas internas de la Cruz Roja Panameña.
- La pérdida de información personal motivo del acceso indebido producto de fuga de información mediante los correos, será puesta en conocimiento de la autoridad competente.

Cualquier empleado y/o voluntario que viole las políticas descritas en este documento o utilice el Correo Electrónico de la Cruz Roja Panameña para cualquier propósito que se juzgue como impropio o irrazonable por la Cruz Roja Panameña, estará sujeto a acciones disciplinarias de acuerdo con las normas internas de la Cruz Roja Panameña (Código de Conducta).

d. Deslinde de responsabilidad

<<La información contenida en este correo es de uso exclusivo de la Cruz Roja Panameña y de carácter confidencial, no se debe leer, copiar, revelar, reenviar o utilizar por personas que no son los destinatarios de este o, sin la autorización del titular de la información. Será responsabilidad del que la difunda, y puede ser objeto de acciones legales. Si ha recibido este correo por error, por favor notifique al remitente y borre el mensaje y cualesquiera adjuntos que contenga>>

9. Seguridad.

Toda la información electrónica (personal u oficial) enviada o almacenada mediante los recursos y las tecnologías de la información y las comunicaciones de la Cruz Roja Panameña son propiedad de la organización. La Cruz Roja Panameña se reserva el derecho a acceder a la totalidad de esa información, incluidos los mensajes de correo electrónico y mensajes de texto por telefonía móvil enviados o recibidos a través de los recursos institucionales, así como el derecho a leerla y tomar medidas al respecto.

Los usuarios tienen la responsabilidad de controlar la seguridad de sus cuentas y contraseñas informáticas.

- En lo relativo a las contraseñas, los usuarios evitarán utilizar palabras o datos que puedan asociarse con ellos (por ejemplo, el nombre o la fecha de nacimiento).
- Deberán memorizar las contraseñas y no escribirlas ni comunicarlas a otras personas.

Los usuarios han de ser conscientes de los peligros que plantean los sistemas de tecnologías de la información y las comunicaciones en lo que atañe a virus y otros programas u elementos dañinos. Deberán tomar todas las precauciones razonables para proteger los recursos informáticos aplicando las medidas siguientes:

- Asegurarse de actualizar periódicamente los recursos informáticos bajo su control para evitar códigos perniciosos.
- Minimizar el uso de dispositivos extraíbles estrictamente a emergencias. En estas emergencias, verificar los dispositivos extraíbles para comprobar que no tienen virus antes de usarlos en los equipos de la Cruz Roja Panameña.

10. Derecho de autor, licencias y programas informáticos.

La política de la Cruz Roja Panameña consiste en adquirir licencias suficientes para que los usuarios lleven a cabo sus funciones. El Departamento de TI regulará las licencias de los programas informáticos normalizados que se facilitan con los equipos de la Cruz Roja Panameña. Todo programa no normalizado que se instale en los ordenadores de la Cruz Roja Panameña deberá contar con la licencia y la autorización correspondiente. Es responsabilidad de los usuarios disponer de la documentación relativa a la licencia.

Los usuarios que deseen instalar programas informáticos en su ordenador deberán contar con previa autorización del departamento de IT y avalado por la Dirección General de la Cruz Roja Panameña.

11. Cumplimiento de normas y procesos.

La Cruz Roja Panameña otorga gran importancia al carácter privado y confidencial de la información, y reconoce el interés de los miembros del personal en proteger contra todo acceso no autorizado la información almacenada en los sistemas de tecnologías de la información y las comunicaciones de la organización. No obstante, existen circunstancias en las cuales los intereses de la organización priman sobre la privacidad del usuario y justifican el acceso de la Cruz Roja Panameña a los recursos informáticos pertinentes sin el conocimiento o el consentimiento del usuario. Entre esas circunstancias se cuentan las siguientes:

- Ante la necesidad de detectar o diagnosticar vulnerabilidades y problemas de los sistemas o la seguridad, o de proteger de cualquier otra forma la integridad de los recursos y las tecnologías de la información y las comunicaciones.
- Ante motivos para considerar que se puede haber incumplido los reglamentos, normas o las políticas de la Cruz Roja Panameña y el acceso a esos sistemas pudiera revelar información pertinente para la investigación de un eventual uso indebido.
- Si el acceso a los sistemas informáticos es necesario para realizar funciones institucionales esenciales de la Cruz Roja Panameña.

12. Sanciones.

Los usuarios tendrán que rendir cuentas por todo incumplimiento de la presente política. La inobediencia de esta u otras políticas, normas, procedimientos y reglamentos conexos darán lugar a medidas disciplinarias con arreglo al Código de Conducta. Si un contratista contraviene las políticas, normas, procedimientos o reglamentos de la Cruz Roja Panameña, esta podrá rescindir el contrato.

La Cruz Roja Panameña se reserva el derecho a recuperar de los “usuarios” todos los gastos en que haya incurrido como resultado del incumplimiento de la presente política (reparación de daños, repatriación u otros).

13. Declaración de Conformidad.

Política de IT, Cruz Roja Panameña, agosto 2024.

DECLARACIÓN DE CONFORMIDAD

Declaro que he recibido, he leído y he comprendido el documento “Seguridad de la información: Política de uso aceptable” de la Cruz Roja Panameña. Comprende que esta política forma parte de las condiciones de empleo y servicio de la Cruz Roja Panameña y me comprometo a acatarla.

Nombre y apellido	Firma	Lugar	Fecha

14. Anexos: Controles de clasificación de la información.

En esta sección figura una sinopsis de los controles pertinentes para los distintos niveles de clasificación de la seguridad. Todos los procedimientos, las normas y las directrices pertinentes en materia de tecnología de la información son de aplicación constante con respecto a todos los datos electrónicos.

Categoría: Muy Reservada		
Vida útil de la información		Controles de información "Muy Reservada"
Uso y modificación	Cambio de formato	No se debe duplicar información en otro formato a menos que se proteja adecuadamente (es decir, se debe preservar la integridad del formato de la información, por ejemplo, mediante archivos PDF no modificable).
Distribución	Transmisión manual de los documentos	Se utilizará un sobre opaco. Se permitirá la entrega únicamente mediante un mensajero aprobado por el propietario del documento o de los datos. Se solicitará acuse de recibido firmado.
	Transmisión electrónica de los datos	Todas las transmisiones de datos se realizarán mediante una aplicación de mensajería autenticada de alta seguridad. No podrán enviarse por correo electrónico ordinario, ya sea institucional o personal. Los datos se transmitirán exclusivamente a destinatarios individuales (es decir, no se usarán listas de distribución) y no se podrá reenviar a otros destinatarios. Se solicitará acuse de recibido electrónico. La información muy reservada no se enviará por facsímil. No se dejará las impresoras desatendidas mientras se imprime documentos de carácter "muy reservado". Los activos de información se imprimirán únicamente a través de una opción de impresión segura.
	Conversaciones orales	Se deben mantener en una habitación totalmente cerrada. A menos que sea imposible, se recomienda no comunicar esos datos por teléfono. La información de índole muy reservada no se debe transmitir a través de sistemas de radiocomunicación. La información se debe borrar de los equipos o pizarras antes de la salir de la sala.
	Copia	Se debe realizar un número mínimo de copias imprescindibles para las necesidades operativas.

Almacenamiento	Almacenamiento físico	Se deben almacenar los documentos en armarios o cajones bajo llave para impedir el acceso no autorizado. Durante los viajes, el viajero debe llevar consigo los datos de carácter muy reservados en todo momento (es decir, no debe facturarlos en el equipaje).
	Almacenamiento electrónico	El acceso debe estar limitado a la cantidad mínima de personas que lo necesiten para ejercer sus funciones oficiales (es decir, según el principio de conocimiento justificado). Se aplicarán sistemáticamente medidas de seguridad (es decir, cifrado de datos). Los datos se almacenarán únicamente en un dispositivo o en una ubicación seguros (por ejemplo, en un USB verificado y cifrado) con las correspondientes limitaciones de acceso. Es necesario guardar una copia de seguridad en una ubicación protegida con un nivel de seguridad y limitaciones de acceso análogas o más rigurosas. Los datos muy reservados no se almacenarán en ubicaciones donde la Cruz Roja Panameña no tenga control sobre ellos y a las que pueda acceder el gobierno (por ejemplo, Dropbox, Google Drive).
Copia de seguridad o de respaldo	Electrónica	El acceso a las copias de seguridad o de respaldo se limitará a lo estrictamente necesario. La recuperación de copias de seguridad o de respaldo solo se permitirá tras una solicitud oficial validada por el propietario de la información. La recuperación de la información contenida en copias de seguridad o de respaldo serán accesibles únicamente para el propietario de la información.
Eliminación	Papel	Se triturará de manera oportuna y segura los documentos definitivos y de trabajo conexos cuya destinación se imponga al culminar el periodo de retención. Se remitirá a los archivos de manera oportuna y segura los documentos definitivos y de trabajo conexos que se deba transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al culminar el periodo de retención.

	Electrónica	Se destruirá físicamente o se reformateará todos los dispositivos cuando culmine el período de retención. Se deberá imprimir los documentos electrónicos que se deban transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al final del periodo de retención y será la versión impresa la que se remita a los archivos de manera oportuna y segura; a continuación, se procederá a destruir físicamente o a formatear el dispositivo electrónico.
Categoría: Reservada		
Vida útil de la información		Controles de información "Reservada"
Uso y modificación	Cambio de formato	La información no se debe copiar en otro formato a menos que se proteja adecuadamente (es decir, se debe preservar la integridad del formato de la información, por ejemplo, mediante archivos PDF no modificables):
Distribución	Transmisión manual de los documentos	Se utilizará un sobre opaco al enviar los documentos (como expedientes de personal) por correo o servicio de mensajería entre las oficinas de la Cruz Roja Panameña (por ejemplo, entre la oficina central, comités y/u oficinas en terreno).
	Transmisión electrónica de los datos	La transmisión electrónica de los datos se podrá realizar mediante el servicio de correo electrónico institucional, previéndose la protección contra el acceso de usuarios no autorizados. Se podrán enviar los datos a listas de distribución. Se podrá reenviar el mensaje electrónico a otros destinatarios, que tengan la necesidad justificada de conocer la información. No se dejará las impresoras desatendidas mientras se imprime documentos de carácter "restringido" o mientras se envían por facsímil. Se solicitará acuse de recibido electrónico.

	Conversaciones orales	Se deben mantener en una habitación totalmente cerrada. A menos que sea imposible, se recomienda no comunicar los datos por teléfono. La información reservada no se debe transmitir por radio. La información se debe borrar de los equipos o pizarras antes de salir de la sala.
	Copia	Se debe realizar el número mínimo de copias imprescindibles para las necesidades operativas.
Almacenamiento	Almacenamiento físico	Se debe almacenar los documentos en armarios o cajones bajo llave para impedir el acceso no autorizado. Durante los viajes, el viajero debe llevar consigo los datos de carácter reservada en todo momento (es decir, no debe facturarlos en el equipaje).
	Almacenamiento electrónico	El acceso debe estar limitado a la cantidad mínima de personas que lo necesiten para ejercer sus funciones oficiales (es decir, según el principio de conocimiento justificado). Los datos solo se almacenarán en un dispositivo o en una ubicación seguros (por ejemplo, un dispositivo USB verificado y cifrado) con las correspondientes limitaciones de acceso. Será necesario guardar una copia de seguridad en una ubicación protegida con un nivel de seguridad y limitaciones de acceso análogas y rigurosas. La información reservada se podrá almacenar fuera de los locales de la Cruz Roja Panameña, siempre y cuando se apliquen controles de seguridad apropiados.
Copia de seguridad o de respaldo	Electrónica	El acceso a las copias de seguridad o de respaldo se limitará a lo estrictamente necesario. La recuperación de la información en copias de seguridad o de respaldo solo se permitirá tras una solicitud validada por los superiores jerárquicos.

Eliminación	Papel	Se triturarán de manera oportuna y segura los documentos definitivos y de trabajo conexos cuya destrucción se imponga al culminar el período de retención. Se remitirá a los archivos de manera oportuna y segura los documentos definitivos y de trabajo conexos que se deba transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al culminar el período de retención.
	Electrónica	Se destruirá físicamente o se reformateará todos los dispositivos cuando culmine el período de retención. Se deberá imprimir los documentos electrónicos que se debe transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al final del período de retención y será la versión impresa la que se remita a los archivos de manera oportuna y segura; a continuación, se procederá a destruir físicamente o a reformatear el dispositivo electrónico.
Categoría: Interna		
Vida útil de la información		Controles de información "Interna"
Uso y modificación	Cambio de formato	Sin limitaciones
Distribución	Transmisión manual de los documentos	Sin limitaciones
	Transmisión electrónica de los datos	Se deberá utilizar direcciones de correo electrónico institucionales (es decir, que acaben en @cruzroja.org.pa) la primera vez que se distribuya la información interna. Sin limitaciones para la impresión o el envío por facsímil.
	Conversaciones orales	Sin limitaciones
	Copia	Sin limitaciones

Almacenamiento	Almacenamiento físico	Se aplica sistemáticamente la política de "escritorio limpio", es decir, no se debe dejar sobre mesas sin supervisión los documentos internos cuando los miembros del personal salgan de la oficina.
	Almacenamiento electrónico	El acceso debe estar limitado a los usuarios internos.
Copia de seguridad o de respaldo	Electrónica	El acceso a las copias de seguridad o de respaldo se limitará a lo estrictamente necesario.
Eliminación	Papel	Los documentos definitivos y de trabajo conexos que se deba destruir al culminar el período de retención se triturarán de manera oportuna y segura. Los documentos definitivos y de trabajo conexos que se deba transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al culminar el período de retención, se remitirán a los archivos de manera oportuna y segura.
	Electrónica	Todos los dispositivos se destruirán o se reformatearán cuando culmine el período de retención. Se deberá imprimir los documentos electrónicos que se deban transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al final de período de retención y será la versión impresa la que se remita a los archivos de manera oportuna y segura; a continuación, se procederá a destruir físicamente o a reformatear el dispositivo electrónico.
Categoría: Pública		
Vida útil de la información		Controles de información "Pública"
Uso y modificación	Cambio de formato	Sin limitaciones
Distribución	Transmisión manual de los documentos	Sin limitaciones

	Transmisión electrónica de los datos	Sin limitaciones para la transmisión electrónica, incluida la impresión y el envío por facsímil, de la información pública.
	Conversaciones orales	Sin limitaciones
	Copia	Sin limitaciones
Almacenamiento	Almacenamiento físico	Sin limitaciones
	Almacenamiento electrónico	Sin limitaciones
Copia de seguridad o de respaldo	Electrónica	Sin limitaciones
Eliminación	Papel	Se triturarán de manera oportuna y segura los documentos finales y de trabajo conexos cuya destrucción se imponga al culminar el período de retención. Los documentos definitivos y de trabajo conexos que se deba transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al culminar el período de retención se remitirán a los archivos de manera oportuna y segura.
	Electrónica	Se destruirá físicamente o se reformateará todos los dispositivos cuando culmine el período de retención. Se imprimirá los documentos electrónicos que se deban transferir a los archivos de la Cruz Roja Panameña para su almacenamiento al final del período de retención y será la versión impresa la que se remita a los archivos de manera oportuna y segura; a continuación, se procederá a destruir físicamente o a reformatear el dispositivo electrónico.

Prohibición de incluir datos sensibles o datos en herramientas de Inteligencia Artificial.










Política de Tecnología de la Información (IT) 2024 vf

Informe de auditoría final

2024-09-20

Fecha de creación:	2024-09-20
Por:	Japhet Santamaria (japhet.santamaria@cuzroja.org.pa)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAAJKrAh_soeAbtFKOmuR0_fh6VuXBeMLeR

Historial de “Política de Tecnología de la Información (IT) 2024 v f”

-  Japhet Santamaria (japhet.santamaria@cuzroja.org.pa) ha creado el documento.
2024-09-20 - 19:20:13 GMT
-  El documento se ha enviado por correo electrónico a Kindelán González (kindelan.gonzalez@cuzroja.org.pa) para su firma.
2024-09-20 - 19:21:36 GMT
-  Kindelán González (kindelan.gonzalez@cuzroja.org.pa) ha visualizado el correo electrónico.
2024-09-20 - 20:35:29 GMT
-  Kindelán González (kindelan.gonzalez@cuzroja.org.pa) ha firmado electrónicamente el documento.
Fecha de firma: 2024-09-20 - 20:37:35 GMT. Origen de hora: servidor.
-  El documento se ha enviado por correo electrónico a Larissa Rodriguez (larissa.rodriguez@cuzroja.org.pa) para su firma.
2024-09-20 - 20:37:36 GMT
-  Larissa Rodriguez (larissa.rodriguez@cuzroja.org.pa) ha firmado electrónicamente el documento.
Fecha de firma: 2024-09-20 - 21:25:31 GMT. Origen de hora: servidor.
-  El documento se ha enviado por correo electrónico a Elías Solís González (elias.solis@cuzroja.org.pa) para su firma.
2024-09-20 - 21:25:32 GMT
-  Elías Solís González (elias.solis@cuzroja.org.pa) ha visualizado el correo electrónico.
2024-09-20 - 21:26:32 GMT
-  Elías Solís González (elias.solis@cuzroja.org.pa) ha firmado electrónicamente el documento.
Fecha de firma: 2024-09-20 - 21:26:48 GMT. Origen de hora: servidor.

✔ Documento completado.

2024-09-20 - 21:26:48 GMT