Cruz Roja
Costarricense

Políticas de Seguridad de la Información y Normas Generales de Tecnologías de la Información

Aprobada según el acuerdo II-4 de la Sesión Ordinaria 20-2023 del Consejo Nacional realizada el 25 de abril de 2024.

Tabla de contenido

1. CONTEXTO

Para garantizar un óptimo nivel de protección de la información, es fundamental abordar integralmente los aspectos administrativos y de control que incumben tanto a la Sociedad Nacional, sus colaboradores, voluntarios y terceros asociados con la Cruz Roja Costarricense. Este enfoque abarca el cumplimiento de todas las normativas y medidas pertinentes para salvaguardar la seguridad y calidad de los datos.

El Área de TI de la Cruz Roja Costarricense es responsable de garantizar el cumplimiento de esta política. En este sentido, llevará a cabo verificaciones periódicas para asegurar que se cumplan tanto las políticas establecidas como las normativas vigentes en materia de Tecnologías de la Información.

Estas acciones se realizarán considerando los recursos financieros, humanos y tecnológicos disponibles en la institución para cumplir con estos objetivos.

2. MARCO NORMATIVO

Esta política se encuentra incorporada al Contrato de Trabajo y es transversal a toda la normativa interna de la Cruz Roja Costarricense, especialmente a la siguiente:

- Código de Conducta.
- Reglamento Disciplinario de la Asociación Cruz Roja Costarricense.
- Reglamento Interno de Trabajo.

3. OBJETIVO

Establecer y desarrollar una política integral de Tecnología y seguridad de la información para la Cruz Roja Costarricense, con el propósito de supervisar y optimizar la gestión tecnológica de la institución.

4. ÁMBITO DE APLICACIÓN

Esta política se aplica a todos los miembros de la Sociedad Nacional; tanto a colaboradores, voluntarios y terceros (proveedores o visitantes).

El incumplimiento de sus disposiciones puede resultar en la apertura de procesos administrativos disciplinarios, sujetos a sanciones de acuerdo con el Reglamento Disciplinario de la Asociación Cruz Roja Costarricense y el régimen de Sanciones Disciplinarias del Reglamento Interno de Trabajo. Además, se podrían establecer otras responsabilidades según lo estipulado por la legislación vigente.

5. DECLARACIÓN

5.1 Generalidades

a. El Área de TI no será responsable de ningún recurso o servicio informático que esté por fuera de los parámetros establecidos en las políticas aquí consagradas.
b. Los activos adquiridos con base a las disposiciones aquí establecidas son propiedad de la Cruz Roja Costarricense (a menos que se indique explícitamente lo contrario) por ende es ésta quien tiene la potestad de intervenir y tomar decisiones en torno a éstos.
c. El Área de TI es la única área competente para avalar técnicamente la contratación de cualquier servicio tecnológico requerido, incluyendo, pero sin limitar, internet, servicios en nube, telefonía, impresión y otros servicios relacionados con tecnologías de información.
d. Ningún usuario está autorizado para alterar las especificaciones de los software y hardware propiedad de la institución.
e. Los recursos y servicios informáticos que provee la Cruz Roja Costarricense son para uso exclusivo de actividades propias de la institución.
f. Cualquier situación no prevista en esta política será resuelta por el Área de TI.

5.2 Uso de recursos y servicios informáticos

5.2.1 Claves y códigos de usuario

a. La cuenta de usuario y su correspondiente código (credenciales de acceso) son esenciales para que la institución pueda verificar y confirmar la identidad de un usuario en sus sistemas informáticos. Al recibir estas credenciales y crear sus propias claves o códigos, así como al emplear datos personales y dispositivos para la autenticación reforzada, se crea un perfil de identificación digital único. Por ende, el usuario reconoce su responsabilidad exclusiva en el manejo de sus credenciales de acceso, datos personales y dispositivos usados como mecanismos de autenticación. Estos elementos son considerados como el equivalente funcional de su identidad tanto para la institución como para terceros relacionados, implicando que cualquier comunicación emitida

utilizando sus credenciales y/o métodos de autenticación se reconoce como firmada electrónica y legalmente atribuible al usuario.

b. Los mecanismos de acceso concedidos a los miembros de la Cruz Roja Costarricense son responsabilidad individual y no deben ser compartidos con terceros, salvo en casos donde exista un requerimiento legal por parte de alguna autoridad competente. En concordancia con lo anterior, se prohíbe a los usuarios compartir contraseñas u otros medios de acceso que pudieran facilitar un uso no autorizado.

c. Cada usuario debe crear sus propias contraseñas y proceder a su actualización cuando el sistema lo solicite, siguiendo las directrices establecidas por el Área de TI en cuanto a los plazos de vigencia de las contraseñas.

d. Las contraseñas de acceso no deben ser compartidas ni registradas en lugares accesibles a terceros, como monitores, carpetas o escritorios; esto para prevenir accesos no autorizados.

e. En caso de extravío de la clave de acceso se debe contactar al Área de TI e identificarse como propietario de la cuenta y código de usuario; esta área define los medios o mecanismos confiables para verificar la identidad del usuario y proceder a la restauración de contraseñas. Una vez validada la identificación del usuario, se genera una clave de acceso temporal y de único uso para que el usuario luego utilice su propia clave de acceso secreta.

5.2.2 Uso de correo electrónico

El correo electrónico se considera una herramienta de trabajo de uso exclusivo para fines laborales o institucionales y la titularidad de este medio es de la CRC, por lo tanto, la persona cruzrojista debe acatar las disposiciones que regulan su uso de acuerdo con el **A01-PI-TI-01-2024** **"Uso del Correo Electrónico Institucional de la Cruz Roja Costarricense"**.

5.2.3 Uso y acceso a internet, canales de comunicación internos y periféricos en red

a. El uso de los servicios de Internet debe ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.

b. Los servicios de Internet deben ser avalados por el Área de TI, únicamente en aspectos técnicos del servicio, velocidades, tipo de conexión o tecnología a utilizar.

c. No es permitido a ningún colaborador, excepto al Área de TI, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).

d. El Área de TI puede analizar y bloquear accesos no permitidos (aquellos que no guarden relación con aspectos de trabajo) que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

e. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deben ser cambiados, excepto por indicaciones del Área de TI.

f. Se habilita el uso de Whatsapp en los equipos institucionales para las personas cruzrojistas que sean voluntarios o asalariados como medio de apoyo para el ejercicio de sus funciones. Con el propósito de mantener la información institucional segura, los usuarios que reciban equipos de la institución deben implementar doble factor de autenticación o verificación en dos pasos, tanto en el dispositivo, como en el ingreso a Whatsapp. En caso de que el uso inapropiado perjudique los intereses de la Asociación Cruz Roja Costarricense, el infractor enfrentará el proceso disciplinario y judicial según corresponda.
g. Las herramientas digitales de comunicación interna serán definidas por el Área de TI. Queda prohibida la divulgación de información confidencial por estos medios sin la autorización de la Jefatura correspondiente del usuario.
h. La persona cruzrojista que requiera utilizar las impresoras en red disponibles en el edificio Central deberá hacer la solitud respectiva en el Área de TI.
i. El Área de TI le debe asignar una contraseña de acceso a las impresoras a cada usuario, por lo que queda bajo responsabilidad de la persona cruzrojista mantener bajo seguridad dicho acceso.
j. Queda prohibido la impresión de archivos personales o de terceras personas.
k. Queda prohibido descargar archivos de música, programas, videos, juegos, contenido pornográfico y cualquier otro tipo de información que no guarde estricta relación con el área profesional. El Área de TI procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.
l. La persona cruzrojista debe siempre verificar la red wifi a la que se conecte sea confiable o institucional.

5.2.4 Software

a. Para la adquisición de software se deben seguir los procedimientos establecidos por el Área de Compras.
b. El Área de TI es el encargado de definir las especificaciones técnicas para la adquisición de cualquier software.
c. Únicamente el Área de TI es el encargado de instalación y brindar acceso de software en el equipo de cómputo de las personas colaboradoras.
d. Los medios de instalación originales o acceso a portales de descarga será custodiados por el Área de TI.
e. El Área de TI define la metodología formal para el desarrollo de software de los sistemas de información y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y estándares aplicables en el desarrollo de sistemas.
f. Para garantizar la integridad y confidencialidad de la información que se administra en el software desarrollado internamente y antes del paso a pruebas, se deben ejecutar las pruebas al desarrollo y contar con la documentación técnica y manuales de usuario respectiva.
g. Los programadores de software no deben conocer las claves utilizadas en ambientes de producción.

h. Los desarrollos y/o modificaciones hechas a los sistemas no deben trasladarse al ambiente de producción si no se cuenta primero con la documentación, la operación y la seguridad adecuada y la aprobación del Área de TI.
i. Queda prohibido la instalación de software adquirido por Cruz Roja Costarricense en equipos computacionales que no sean propiedad de la institución.

5.2.5 Hardware

a. Para la adquisición de software se deben seguir los procedimientos establecidos por el Área de Compras.
b. Los dispositivos y cualquier otro activo tecnológico de la Cruz Roja Costarricense, se regula por las disposiciones establecidas en las **A02-PI-TI-01-2024 "Condiciones de uso de las herramientas tecnológicas".**
c. Los activos tecnológicos pueden disponerse fuera de las instalaciones de Cruz Roja Costarricense, previo cumplimiento y verificación del siguiente requisito autorizado por el Área de TI:

- Cada colaborador (a) debe llenar la boleta de salida de activos la cual es firmada y almacenada en un archivo por la jefatura correspondiente o el administrador (a) del comité.

d. Las personas cruzrojistas deben firmar la boleta de entrega formal de los activos tecnológicos y estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento; así como contar con un espacio físico adecuado para el equipo. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Área de TI para que se proceda a su revisión.
e. Las personas cruzrojistas deben desconectar el fluido eléctrico de computadoras y algún otro dispositivo que este a su cargo en periodos de descanso, esto como medida de seguridad y no sobre carga los equipos tecnológicos.
f. Queda totalmente prohibido que las personas cruzrojistas reparen o desarmen algún equipo computacional, de tener alguna complicación es importante que siempre lo reporten al Área de TI.
g. Las personas cruzrojistas deben de respaldar la información que consideren sensible y mantenerla en la nube necesario, esto para evitar alguna pérdida de información.
h. Las personas cruzrojistas deben respetar los sellos de garantía que vienen adheridos a los equipos y no despegarlos.
i. Las personas cruzrojistas tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.

j. Es responsabilidad del Área de TI valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.
k. Las ampliaciones, modificaciones o adquisición de equipo de cómputo, así como la actualización y compra de software, se hacen únicamente con el aval por del Área de TI.
l. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del Área de TI, el cual debe velar por su uso y cuidado.
m. El Área de TI debe asegurar en su infraestructura tecnológica, un control de gestión de cambios realizados en los sistemas, así como la infraestructura tecnológica.
n. El Área de TI determina cuál es el antivirus oficial y realiza la instalación en los equipos institucionales cuando se cuente con la debida licencia.
o. El Área de TI es la responsable de documentar y aplicar procedimientos para nombrar los equipos. Se debe utilizar la configuración que considere óptima para la identificación de los equipos.
p. El Área de TI tiene un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales En caso de robo de los equipos tecnológicos asignados debe ser reportarlo inmediatamente al Área de TI y éste gestiona con la administración el procedimiento a seguir.

5.2.6 Manejo de desechos de los medios tecnológicos

a. Los equipos electrónicos para desechar deben ser revisados por el Área de TI, generando un acta de desecho la cual debe ser entregada a la Unidad de Activos Fijos como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.

5.3 Control de la información

a. Todas las personas cruzrojistas están obligadas a gestionar toda la información, datos, documentos y demás material institucional exclusivamente a través de la red o mediante una infraestructura en la nube, como Office 365 (incluyendo Microsoft OneDrive y Microsoft SharePoint).
b. Las personas cruzrojistas deben informar por correo electrónico al Área de TI o bien a su jefatura directa toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos, intentos de intromisión correos electrónicos sospechosos y no deben distribuir este tipo de información interna o externamente. El Área de TI debe llevar a cabo una evaluación remota del equipo y, según su criterio técnico y conclusiones, puede solicitar al usuario que traslade el equipo a las instalaciones físicas de este departamento.

c. Toda persona cruzrojista que utilice los recursos de los sistemas informáticos de la institución, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como confidencial.

d. Las personas cruzrojistas asalariados y voluntarios que por motivo atribuible a la Asociación no tengan asignado equipo tecnológico institucional, podrán hacer uso del equipo personal, hasta que la institución se los facilite, siempre y cuando cumplan los lineamientos de esta política en cuanto al manejo de la información confidencial, privada y datos sensibles que pudiesen perjudicar el fin que persigue la institución. En caso de corroborarse un incumplimiento, el colaborador podrá ser susceptible a un proceso sancionatorio.

e. Las personas cruzrojistas deben mantener bloqueada su computadora cuando no se encuentren en su estación de trabajo, con el fin de velar por la integridad y confidencialidad de su información y de su área.

f. El Área de TI es responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo de la Cruz Roja Costarricense.

g. El Área de TI establece los mecanismos adecuados para el control, verificación y monitoreo de cambios en password, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información. Si es necesario y de acuerdo con las Políticas internas, una jefatura puede solicitar justificadamente al área de TI bloquear los accesos de un usuario específico.

h. La persona cruzrojista es el responsable de realizar los respaldos de su información y mantenerlos resguardados en los medios adecuados que le permita una recuperación segura en caso de algún daño al equipo. En caso de las aplicaciones cliente-servidor el responsable de realizar los respaldos es el administrador o encargado de base de datos del Área de TI, quien debe realizar un acompañamiento a los colaboradores para el uso adecuado de medios cloud como opción de respaldo.

i. La responsabilidad de la seguridad de la información y de la protección de la infraestructura tecnológica es un compromiso de toda persona cruzrojista, las jefaturas de área o de comités, son responsables de velar por el cumplimiento por parte de las personas cruzrojistas, de las medidas de protección de la información y del adecuado uso de las herramientas tecnológicas establecidas en esta Política y demás políticas relacionadas.

j. El Área de TI es el responsable de liderar la estrategia de seguridad de la información y de crear los lineamientos y medidas necesarias para lograr un ambiente de trabajo seguro a través de los medios tecnológicos disponibles.

5.4 Control de datos

a. Todos los datos de Cruz Roja Costarricense deben de clasificarse dentro de las siguientes categorías para los datos sensibles: CONFIDENCIAL, PRIVADO, y para los datos no sensibles la categoría es PÚBLICO.
b. Las jefaturas de los departamentos son las encargadas de brindar acceso de la información a terceras personas.
c. Cuando se consolida la información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y se debe clasificar con el máximo nivel de restricción que contenga la misma.
d. El Área de TI, mediante un software debe controlar el acceso de medios extraíbles (USB, discos duros externos) para evitar la fuga de la información institucional.
e. Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los colaboradores de la institución, durante el tiempo que dure su relación laboral, son de propiedad exclusiva de Cruz Roja Costarricense.
f. Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para eso, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.
g. Los colaboradores no deben destruir, copiar o distribuir los archivos de Cruz Roja Costarricense sin los permisos respetivos de las jefaturas directas.
h. Toda divulgación de información confidencial o privada a terceras personas debe estar acompañada por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada.
i. Es responsabilidad de la persona cruzrojista evitar en todo momento la fuga de información que se encuentre almacenada en los equipos que tenga asignados caso contrario y de comprobarse la falta se expone a un proceso disciplinario y eventuales sanciones.
j. Las personas cruzrojistas con firma digital certificada deben de disponer en sus dispositivos de todos los drivers y lectores para el correcto funcionamiento de esta.
k. El formato único para firmar digitalmente es en documento PDF pueden utilizar las aplicaciones:

- Firmador Libre.
- Sistema Gaudí (sistema para firmar digitalmente) emitido por el Banco Central de Costa Rica.
- Adobe Reader.
- Software avalado por Informática que cumpla con el estándar del Banco Central de Costa Rica para la generación correcta de la firma electrónica. Después de estampada la firma con el certificado digital es responsabilidad del firmante verificar que la firma digital cumpla con todos los atributos establecidos en el inciso i.

l. Es responsabilidad de las personas cruzrojistas verificar que todos los documentos internos y externos que estén firmados con certificado digital cumplan con integridad, autenticidad y sellado en el tiempo, además que el certificado se encuentre vigente al momento de la firma, lo anterior para garantizar la validez jurídica según lo indicado en la Ley 8454 de certificados, firmas digitales y documentos electrónicos.

5.4.1 Manejo de Base de Datos Institucionales

a. Todo acceso a las bases de datos de Cruz Roja Costarricense debe ser administrado por el Área de TI y los permisos se otorgan según las funciones.
b. El Área de TI vela porque la base de datos que sea instalada cuente con los controles de seguridad que garanticen la confiabilidad de la información.
c. El Área de TI establece los planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.
d. Las Bases de Datos Institucionales deben estar debidamente inscritas a la agencia de protección de datos de los habitantes y cumplir la Ley de Protección de Datos y su reglamento.
e. Toda migración de base de datos debe ser realizada por el encargado de las bases de datos del Área de TI o personal externo que corresponda bajo la supervisión del Área de TI.
f. Todas las bases de datos que estén en soporte digital o en soporte físico se encuentran protegidas por derechos de autor cuya titularidad le pertenece a la Cruz Roja Costarricense.

5.4.2 Normativa interna de privacidad y tratamiento de datos personales

a. De acuerdo con lo dispuesto en la Ley 8968 Ley de Protección de la Persona frente al tratamiento de sus datos personales, así como el Reglamento N° 37554-JP Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (en adelante, "La Ley"), en esta normativa se regula y se establecen las medidas y procedimientos necesarios para garantizar la protección de datos de las personas físicas (en adelante, "Usuarios") que comparten sus datos personales con la Asociación Cruz Roja Costarricense (en adelante, "Responsable" o "CRC"). Link acceso a normativas

5.5 Contratos para el acceso a la información por parte de terceros así como la contratación de servicios prestados por éstos

a. El acceso a la información por parte de terceros requiere de contratos de confidencialidad previamente establecidos por la Dirección Jurídica o de la solicitud formal de la jefatura para la asignación de roles o privilegios que los faculten para la consulta controlada.
b. En la contratación de servicios a terceros se debe establecer cláusulas específicas sobre la confidencialidad de la información.

c. Existen formatos de contratos y acuerdos enfocados en la seguridad de datos, los cuales regulan la colaboración entre la Cruz Roja Costarricense y otras entidades. Además, se establecen términos específicos para el tratamiento de datos con proveedores. Link acceso contratos, Acuerdos y Consentimientos Informados

5.6 Control de dispositivos móviles

a. El uso de los dispositivos móviles utilizados en la ejecución de las funciones de las personas cruzrojistas, se regula por las disposiciones aquí establecidas y por lo estipulado en las **A02-PI-TI-01-2024 Condiciones de uso de las herramientas tecnológicas.**
b. Todos los dispositivos móviles asignados por la Cruz Roja Costarricense a las personas cruzrojistas, deben utilizar autenticación multi factor (autenticación reforzada) para lograr acceso al uso del dispositivo. Siempre que el dispositivo o las licencias de software adquiridos por la Cruz Roja, permitan habilitar esta funcionalidad.
c. Se debe reportar la pérdida, robo o daño de dispositivos de forma inmediata al conocimiento del hecho.
d. Deben tener un sistema operativo obtenido por canales oficiales o instalado de fábrica, así mismo, no deberán ligarse cuentas personales si no únicamente institucionales.
e. Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.
f. Se debe implementar, para los dispositivos que lo soporten, instrumentos y herramientas técnicas (hardware, software) que permitan bloquear y/o borrar la información de forma remota.
g. El Área de TI será el encargado de definir los requerimientos técnicos de acuerdo con los perfiles establecidos por el departamento, TI será el encargado de la configuración o reconfiguración de celulares.
h. Los equipos celulares, son gestionados (Plaqueo de activos, registro en los sistemas, documentación del proceso, custodia, desecho) por el área de Activos Institucionales, en conjunto con la Bodega Central.
i. Las personas cruzrojistas autorizados para el uso de celulares institucionales serán definidas por la Gerencia General.
j. Queda prohibido a aquellas personas cruzrojistas a quienes se les ha asignado un servicio de dispositivos móviles y líneas de telecomunicación lo siguiente:

- Modificar la configuración del servicio en cuanto a número telefónico, servicios o cualquier otra forma que dificulte o impida mantener el control adecuado sobre su uso.
- Ceder o prestar el aparato, sus accesorios o el derecho de uso a terceras personas, formal o informalmente, ya sea temporal o permanentemente, para fines y acciones diferentes a los intereses de esta Asociación.
- Utilizar el aparato o sus accesorios en otras tareas o actividades diferentes a las asignadas debido a su cargo.

k. En caso de robo del dispositivo tecnológico, de sus accesorios o de ambos, la persona cruzrojista responsable del equipo debe informar al Área de TI a más tardar el día hábil siguiente para que se proceda a solicitarla suspensión del servicio a la empresa proveedora, así mismo, debe presentar la respectiva denuncia ante el Organismo de Investigación Judicial (OIJ).

l. En caso de daño de los dispositivos móviles, si se comprueba que son por un uso inadecuado por parte del usuario, podría generarse responsabilidad administrativa, civil o disciplinaria. Además la persona cruzrojista debe cubrir el costo de la reparación o costo proporcional al monto indicado en los libros de saldos contables, aplicándose la respectiva depreciación.

m. La asignación de dispositivos móviles y líneas de telecomunicación no se considera como parte del salario, por lo que la persona cruzrojista no tendrá derecho alguno a cobrar el uso del teléfono como parte del pago por concepto de prestaciones laborales. La asignación de este servicio no constituye un beneficio personal.

n. La persona cruzrojista que fuese trasladado o removido de su cargo, o bien en el momento en que concluyan las circunstancias que motivaron la asignación del servicio de dispositivos móviles y líneas de telecomunicación, debe hacer la devolución del equipo en presencia de su jefatura inmediata, personeros del Área de TI, Talento Humano.

o. Cuando por condiciones de distancia no puedan concurrir los personeros descritos con anterioridad, la entrega del equipo se debe hacer en presencia de la jefatura inmediata correspondiente donde labora el usuario del dispositivo, quien verifica mediante acta proveída por el Área de TI las condiciones de recibo. Posteriormente, remite el dispositivo en un plazo máximo de cinco días hábiles al Área de TI. De existir un atraso en la devolución por responsabilidad de la persona cruzrojista a quien se le hubiere asignado el servicio, las multas o demás erogaciones que proceda cancelar al proveedor quedarán bajo su exclusiva responsabilidad.

p. Las tarifas para el pago de los servicios de dispositivos móviles y líneas de telecomunicación que sean propiedad de esta Asociación se regirán por los montos aprobados por la Gerencia.

q. La Gerencia o la jefatura directa del funcionario puede retirar su uso unilateralmente en cualquier momento y dejar sin efecto la asignación de dispositivos móviles y líneas de telecomunicación, cuando lo considere necesario.

5.7 Control de equipos tecnológicos en modalidad teletrabajo

a. Los dispositivos y cualquier herramienta tecnológica suministrada por la Cruz Roja Costarricense para la ejecución de las funciones laborales en modalidad de teletrabajo; se regula por las disposiciones aquí establecidas y por lo estipulado en las **A02-PI-TI-01-2024 Condiciones de uso de las herramientas tecnológicas.**

b. La computadora o dispositivos tecnológicos brindados por la institución a las personas que realicen teletrabajo deben de contar con una protección

antivirus. Es responsabilidad del usuario avisar al Área de TI si su computadora no cuenta con antivirus para proceder a instalarlo de forma inmediata.

c. Las personas que realicen teletrabajo deben conectarse a la red institucional únicamente por el VPN instalado por el Área de TI y ésta debe habilitar mecanismos de autenticación reforzada o de doble factor, siempre que la licencia o los mecanismos técnicos necesarios hayan sido adquiridos por la Cruz Roja para la habilitación de esta funcionalidad.

d. Las personas que realicen teletrabajo deben manejar la mayoría de su información en la red o una infraestructura cloud como office 365 (Microsoft One Drive, Microsoft SharePoint).

e. Se deben aplicar las siguientes medidas preventivas desde el lugar donde realicen el teletrabajo:

- Concluir las sesiones activas de cualquier sistema informático al finalizar las tareas.
- Proteger el equipo contra usos no autorizados mediante un mecanismo de bloqueo de seguridad autorizado por la Institución.
- Cerrar la conexión con los servidores.
- Cerrar conexiones de VPN y sistemas asociados a la institución.

f. Deben contar con el requisito básico de una conexión mínima de internet de 5 Mbps**.** Cuando no es posible utilizar la red doméstica o cualquier otra red considerada segura como alternativa; las persona cruzrojista debe utilizar la red de datos móvil 4G siempre evitando la conexión a redes wifi públicas inseguras.

g. En caso de que las personas que realicen teletrabajo tienen inconvenientes por falta de fluido eléctrico, ésta debe comunicarlo inmediatamente a su jefatura, para coordinar lo pertinente en el actuar para el cumplimiento de los objetivos trazados por el departamento y la institución.

h. Las personas que realicen teletrabajo deben estar de forma "online" y/o "disponible" en los horarios respectivos de trabajo según la modalidad que la institución y su jefatura directa le hayan designado.

i. En caso de que la persona cruzrojista deba realizar teletrabajo en un espacio público con tránsito continuo de personas, debe seguir las indicaciones del inciso e de esta sección. Además, debe asegurarse de no desplegar en la pantalla de su computadora información sensible o confidencial que terceros puedan ver, ni de extender documentos o cualquier otra información importante sobre la mesa de trabajo.

j. La persona colaboradora debe procurar ubicarse en sitios con un grado razonable de privacidad, evitando que la pantalla este expuesta a terceros o a cámaras de vigilancia. Si por las circunstancias de las funciones debe trabajar de forma continua en espacios públicos con su computadora de trabajo, debe utilizar en la pantalla de su dispositivo un filtro de privacidad.

5.8 Conductas prohibidas en el uso de la información y las herramientas tecnológicas

a. El uso de la información a la que tiene acceso la persona cruzrojista, así como el uso de las herramientas de trabajo y de la infraestructura tecnológica deberá apegarse a lo establecido en el Contrato de Trabajo, Código de Conducta y demás Políticas internas, por lo tanto, son conductas totalmente prohibidas por estos las siguientes:

i. Apoderarse, acceder, modificar, alterar, suprimir, intervenir, interceptar, abrir, entregar, vender, remitir o desviar de su destino sin autorización del titular, documentación o comunicaciones dirigidas a otra persona.
ii. Apoderarse, modificar, interferir, acceder, copiar, transmitir, publicar, difundir, recopilar, inutilizar, interceptar, retener, vender, comprar, desviar para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica.
iii. Grabar sin consentimiento manifestaciones de terceros no destinadas al público y que no le están dirigidas.
iv. Suplantar la identidad de una persona física o jurídica.
v. Alterar o modificar cualquier sistema informático de la institución o utilizar datos fraudulentos en un sistema informático para procurar un beneficio económico. (Estafa informática)
vi. Destruir, inutilizar, suprimir, modificar, desaparecer o dañar cualquier sistema informático, información, base de datos, dispositivo electrónico o herramienta tecnológica propiedad de la CRC.
vii. Impedir, obstaculizar, alterar, entorpecer o inutilizar el acceso o funcionamiento de un sistema informático o de la información contenida en este.
viii. Manipular un sistema informático o cualquier dispositivo electrónico para apoderarse, transmitir, copiar, modificar, destruir, utilizar, bloquear o reciclar información sensible o confidencial.
ix. Instalar sin autorización, virus o programas informáticos maliciosos en un sistema informático propiedad de la CRC.
x. Crear virus, código malicioso o malware.
xi. La adquisición de equipo de cómputo que no tenga el visto bueno del Área de TI.
xii. Suplantar sitios web.
xiii. Facilitar la comisión de delitos mediante un sistema informático, dispositivo electrónico o herramienta tecnológica propiedad de la CRC.
xiv. Difundir, almacenar o descargar cualquier tipo de pornografía.

b. La sospecha fundada de cualquier de estas conductas dará apertura a una investigación interna. Así mismo una vez comprobados los hechos se procederá con las sanciones disciplinarias internas y la denuncia penal correspondiente.

c. Las personas cruzrojistas no deben intentar sobrepasar los controles de los sistemas, examinar las computadoras y redes de la Cruz Roja Costarricense en busca de archivos de otros sin su autorización, introducir o instalar intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

d. Las personas cruzrojistas no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación.
e. Las personas cruzrojistas no deben destruir o copiar los archivos, o documentación relacionada con la Cruz Roja Costarricense sin los permisos respectivos.

6. RESPONSABILIDADES

6.1 Órganos de Gobierno

a. Fiscalizar que toda la estructura de la Sociedad Nacional cumpla lo dispuesto en las políticas de Seguridad de la Información y Normas Generales de TI.
b. Promover el desarrollo de la política en las normativas de la Sociedad Nacional.

6.2 Órganos de Gestión

a. Aplicar y garantizar la ejecución de la Política de Seguridad de la Información y Normas Generales de TI.
b. Aplicar la normativa sancionatoria establecida en las políticas en pro de garantizar el cumplimiento.
c. Verificar que el personal asalariado y voluntario reciban la capacitación sobre la política.

6.3 Voluntarios y Asalariados

a. Aplicar en el ámbito de trabajo lo establecido en esta política.
b. Denunciar el incumplimiento de la política con el órgano fiscalizador inmediato.
c. Contribuir con el ejemplo el cumplimiento de las directrices fundamentadas en esta política.

6.4 Supervisión de políticas Políticas y Normas Generales de TI

La supervisión del cumplimiento de esta política queda a cargo Área de Tecnologías de la Información; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y las normativas vigentes en materias de tecnologías de información.