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

Cruz Roja Costarricense

Gestionado por	Departamento de Tecnologías de la Información
Posición responsable	Jefatura
Información de contacto	soporte@cruzroja.or.cr
Fecha de aprobación	9 julio del 2022
Aprobado por	Acuerdo del Consejo Nacional xxxxxxx
Versión	Versión 1
Próxima fecha de revisión	Julio 2023.

Creación

Ing. Milagro Pérez Valerín. Jefatura de Departamento de Tecnologías de Información
Lic. Celimo Fuentes Bravo. Asesor Legal. Dirección Jurídica.

Revisión y aportes

Ing. Walter Fallas Bonilla. Subgerente Administrativo.
Lic. Jose Gerardo Barahona Vargas. Director Jurídico.
MAP. Alejandra Mora Segura. Jefatura Departamento de Planificación.

Principios Fundamentales

Siendo que Costa Rica es Estado parte de la conferencia de Ginebra y, de acuerdo con la XX Conferencia Internacional de la Cruz Roja, celebrada en Viena en 1965 y los Estatutos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, aprobados por la XXV Conferencia Internacional de la Cruz Roja celebrada en Ginebra en 1986, los principios fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja son:

Humanidad. El Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, al que ha dado nacimiento la preocupación de prestar auxilio, sin discriminación, a todos los heridos en los campos de batalla, se esfuerza bajo su aspecto internacional y nacional, en prevenir y aliviar el sufrimiento de los hombres en todas las circunstancias. Tiende a proteger la vida y la salud, así como a hacer respetar la persona humana. Favorece la comprensión mutua, la amistad, la cooperación y la paz duradera entre todos los pueblos.

Imparcialidad. No hace distinción de nacionalidad, raza, religión, condición social, ni credo político. Se dedica únicamente a socorrer a los individuos en proporción con los sufrimientos, remediando sus necesidades y dando prioridad a las más urgentes.

Neutralidad. Con el fin de conservar la confianza de todos, el Movimiento se abstiene de tomar parte en las hostilidades y, en todo tiempo, en las controversias de orden político, racial, religioso e ideológico.

Independencia. El Movimiento es independiente. Auxiliares de los poderes públicos en sus actividades humanitarias y sometidas a las leyes que rigen en los países respectivos, las Sociedades Nacionales deben, sin embargo, conservar una autonomía que les permita actuar siempre de acuerdo con los principios del Movimiento.

Voluntariado. Es un Movimiento de socorro voluntario y de carácter desinteresado.

Unidad. En cada país sólo puede existir una sociedad de la Cruz Roja o de la Media Luna Roja, que debe ser accesible a todos y extender su acción humanitaria a la totalidad del territorio.

Universalidad. El Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, en cuyo seno todas las sociedades tienen los mismos derechos y el deber de ayudarse mutuamente, es universal.

Terminología, siglas o símbolos

- **CRC:** Cruz Roja Costarricense.
- **PGA:** Procedimiento de Gestión Administrativa serán aquellos que describan los pasos o la rutina para llevar a cabo las tareas de los procesos administrativos, permitiendo una acción coordinada entre las diferentes unidades de la organización y sus funciones internas. Se definen como la secuencia de operaciones de oficina para captar y procesar información que permita desarrollar efectivamente los procesos y generar datos para la toma de decisiones y el control.
- **TH:** Talento Humano
- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **T.I:** Tecnologías de la Información.
- **Data Center:** Se denomina Centro de Proceso de Datos al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- **Password:** Contraseñas.
- **Servidor:** Un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.
- **VPN:** "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas.
- **WIFI:** Tecnología que permite conectar diferentes equipos informáticos a través de una red inalámbrica de banda ancha.
- **USB:** Universal Serial Bus), más conocido por la sigla USB, es un bus de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.
- **Backup:** Copia de seguridad de los datos realizada en un soporte de almacenamiento adecuado (un disco duro externo, por ejemplo).
- **Nube o cloud:** La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o simplemente «la nube», es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.
- **PDF:** Es un formato de almacenamiento para documentos digitales independientes de plataformas de software o hardware. Este formato es de tipo compuesto**.**
- **PC:** Computadora
- **Switches:** Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.
- **Router**: Enrutador (del inglés router) o encaminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.
- **Browser:** Navegador de internet.
- **Cookies:** Una cookie es un fichero de datos que una página web le envía a tu ordenador cuando la visitas.
- **Chats:** Comunicación en tiempo real que se realiza entre varios usuarios cuyas computadoras están conectadas a una red, generalmente Internet; los usuarios escriben mensajes en su teclado, y el texto aparece automáticamente y al instante en el monitor de todos los participantes.
- **Red:** Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos)
- **MBPS:** Un megabit por segundo es una unidad que se usa para cuantificar un caudal de datos equivalente a 1000 kb/s.
- **Online**: Que está disponible o se realiza a través de internet o de otra red de datos.
- **MIFI:** El MiFi es un router 4G inalámbrico que cuenta con una batería interna para no tener que depender de una fuente de alimentación y puede dar conexión a distintos dispositivos a la vez. Su nombre viene dado por la abreviatura de: Mi Wifi. Cada vez encontramos más tecnologías y formas de tener conexión a Internet.

Tabla de Contenido

Contenido

1 Contexto

Cubrir todos los aspectos administrativos y de control que deben de ser cumplidos por la Sociedad Nacional, colaboradores, voluntarios y terceros que laboren o tengan relación con la Cruz Roja Costarricense, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información.

El cumplimiento de esta política queda a cargo del Departamento de Tecnologías de la Información de la Cruz Roja Costarricense, razón por la cual este departamento verificará en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materia de Tecnologías de la Información y Comunicación.

2 Marco Normativo

- Código de Conducta.
- PGA-TH-02 Desvinculaciones del personal de CRC**.**
- Reglamento Disciplinario de la Asociación Cruz Roja Costarricense.
- Reglamento de compras interno de la Cruz Roja.
- Reglamento Interno de Trabajo

3 Objetivo

Establecer la política de seguridad de la información de la Cruz Roja Costarricense, con el fin de regular la gestión tecnológica de la Institución.

4 Ámbito de Aplicación

La política es aplicable a todos los personeros de la Sociedad Nacional, colaboradores, voluntarios y terceros (proveedores o visitantes).

El incumplimiento de esta política podría originar la apertura de procesos administrativos disciplinarios para establecer sanciones según el Reglamento Disciplinario de la Asociación Cruz Roja Costarricense, sin perjuicio de establecer cualquier otro tipo de responsabilidad que conforme el ordenamiento jurídico le sean aplicables.

5 Declaración

5.1 Seguridad Institucional

5.1.1 Claves y códigos de usuario

a. Los mecanismos de acceso que les sean otorgados a los cuzrojistas son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal emitido por la Dirección Jurídica, Procesos Disciplinarios o bien el Juzgado competente. De acuerdo con lo anterior, los usuarios no deben compartir las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.
b. Los cruzrojistas son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal de acceso a todos los sistemas de Cruz Roja.

5.1.2 Control de información

a. Los cruzrojistas deben informar por correo electrónico o el medio determinado por el departamento de TI o bien su jefatura directa toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.
b. Los 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.
c. Los 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.
d. Los cruzrojistas no deben destruir o copiar los archivos, o documentación relacionada con la Cruz Roja Costarricense sin los permisos respectivos.
e. Todo cruzrojista que utilice los recursos de los sistemas 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 crítica.
f. Los cruzrojistas deberán de mantener bloqueada su computadora cuando se levanten de su estación de trabajo, ya que es responsabilidad de cada cruzrojista velar por la integridad y confidencialidad de sus funciones y sus departamentos respectivos.
g. El Departamento de TI es el 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.
h. El Departamento de TI establecerá 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.
i. Para evitar situaciones de peligro para Cruz Roja Costarricense se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a un mes, para lo cual debe informar la jefatura respectiva.
j. El colaborador de TI no cambiará ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura se bloqueará los accesos de un usuario específico.
k. Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números. El período lo establecerá el Departamento de TI, dependiendo de la sensibilidad de la información.
l. El cruzrojista no debe dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio).
m. Cuando el cruzrojista olvide u extravíe su clave de acceso, deberá acudir al Departamento de Tecnología de Información e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que el Departamento de TI defina para la restauración de contraseñas.
n. La clave de acceso nunca debe ser compartida o revelada; hacer esto responsabiliza al usuario que prestó su clave de acceso y todas las acciones que se realicen con la misma.

o. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar del primer nombre, punto y seguido del primer apellido. En caso de repetirse los formatos se agregará la primera letra del segundo apellido.
p. El administrador del sistema de información asignará la clave de acceso al usuario.
q. Para otorgarle acceso a las diferentes aplicaciones del sistema, de acuerdo con las funciones que debe desempeñar el colaborador, la jefatura correspondiente deberá hacer la solicitud formal al encargado de TI.
r. Los Data Center deben estar completamente cerrados y con una única puerta de acceso, la cual deberá permanecer siempre cerrada. Las llaves de acceso estarán en custodia del personal del Departamento de TI.
s. El cruzrojista será 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 será el administrador o encargado de base de datos del Departamento de Tecnologías de Información. El departamento realizará un acompañamiento a los colaboradores para el uso adecuado de medios cloud como opción de respaldo.
t. Todo visitante que ingrese a las instalaciones de la Cruz Roja con equipo de cómputo personal deberá de ser registrado con el guarda de seguridad para poder ingresar con el mismo a la institución.
u. Toda empresa contratada para labores de mantenimiento en los equipos de la sala de servidores de TI deberá coordinar con anticipación la visita con el personal de TI para verificar su disponibilidad.
v. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado. Deberá utilizarse para el cableado de red la certificación vigente en el momento que se instalen nuevas conexiones.
w. El departamento de TI, con el área de infraestructura debe de asegurar en los sistemas de información, así como en los servidores, el correcto seguimiento e implementación de los logs para un seguimiento adecuado de una auditoria.

5.1.3 Colaboradores de nuevo ingreso

Todo ingreso de cruzrojistas nuevos debe de notificarse por escrito al departamento de TI **con tres días de anticipación** esto con el fin de que se creen, habiliten o modifiquen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes. Todos los colaboradores deben de recibir la inducción a estas políticas para darles a conocer las obligaciones y las sanciones que pueden incurrir en caso de incumplimiento.

5.1.4 Salida o despidos de colaboradores

En caso de que el cruzrojista decida la salida por su propia cuenta o bien el despido de este, se le debe de informar al departamento de TI por escrito para el retiro y bloqueo de todos los accesos de la institución tomando en cuenta el PGA-TH-02 Desvinculaciones del personal de CRC.

5.1.5 Acceso físico a las áreas de Acceso restringido

Las oficinas del Departamento de Tecnologías de la Información, Dirección Jurídica, Financiero Contable, Auditoria y Gerencias son de acceso restringido y deben de ser rotuladas en conjunto con el área de salud ocupacional, dadas las características y complejidad de la información que manejan. Por lo tanto, deben de llevar una bitácora de ingresos de usuarios ajenos a las dependencias mencionadas anteriormente.

5.1.6 Espacio de Trabajo Seguro

a. El cruzrojista debe asegurarse que en su estación de trabajo no tenga a exposición documentación de carácter confidencial. Así mismo debe de asegurar que la información impresa debe de estar almacenada en un lugar seguro y con clave. Para lo cual el departamento de TI hará un proceso de concientización mediante charlas, infografías y explicación de esta política.
b. El cruzrojista deberá asegurar siempre el bloqueo de su computadora a la hora de levantarse de su estación de trabajo.

c. El cruzrojista no debe de dejar contraseñas a la vista de otros usuarios.
d. El cruzrojista debe siempre verificar la red wifi a la que se conecte sea confiable o institucional.
e. Verificar el uso de VPN en modalidad de Teletrabajo si el puesto de trabajo lo requiere.

5.2 Control de Software

Los cruzrojistas deben seguir los siguientes lineamientos para controlar el software instalado en los dispositivos móviles y computadoras para evitar la piratería y el software malintencionado.

5.2.1 Administración de Software

a. Cruz Roja Costarricense debe contar con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento y el entregado. Igualmente, todo el software y la documentación de este que posea Cruz Roja Costarricense incluirán avisos de derechos de autor y propiedad intelectual.
b. Los ambientes de desarrollo de sistemas internos, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad.
c. Los programas que se encuentren en el ambiente de producción de Cruz Roja Costarricense se modificarán únicamente por el personal autorizado de TI.
d. Los medios de instalación originales o acceso a portales de descarga será custodiados por TI.
e. Únicamente el departamento de TI es el encargado de instalación de software en el equipo computacional de los colaboradores.
f. Queda prohibido la instalación de software adquirido por Cruz Roja Costarricense en equipos computacionales que no sean propiedad de la institución.

5.2.2 Adquisición de Software

a. La Proveeduría en conjunto con el departamento de Tecnologías de Información procederán con la compra del software mediante los procedimientos de adquisición de bienes y servicios establecidos en la legislación costarricense publicada para este fin.
b. El departamento de Tecnologías de la Información será el encargado de definir las especificaciones técnicas para la adquisición mediante fondos propios o públicos, donación, venta, reubicación, préstamo, cesión, remate o por cualquier medio de software.
c. El software adquirido tendrá como fin proteger los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos otorgados por TI.

5.2.3 Desarrollo de Software

a. Cruz Roja Costarricense con su departamento interno de TI definirá 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.
b. Para garantizar la integridad y confidencialidad de la información que administrará el software desarrollado internamente y antes del paso a pruebas, se deberán ejecutar las pruebas al desarrollo y contar con la documentación técnica y manuales de usuario respectiva.
c. Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción.
d. Los desarrollos y/o modificaciones hechas a los sistemas no deberán 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 sistemas o jefatura de TI.

5.2.4 Pruebas de Software

a. El departamento de TI deberá hacer las pruebas en representación de los usuarios finales.
b. El área de desarrollo de sistemas deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual deberá ser revisado para encontrar códigos mal intencionados y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para luego ser compilado e iniciar las pruebas correspondientes.
c. Los tipos de pruebas deberán ser previamente establecidos. Para garantizar la integridad de la información en producción éstas deberán ser debidamente planeadas, ejecutadas, documentadas y controlados sus resultados, con el fin de garantizar la integridad de la información en producción. Además, el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de producción.

5.2.5 Implantación de Software

a. Antes de implementar el software en producción se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. Deberá existir un cronograma de puesta en producción con el fin de minimizar el impacto de este.

5.2.6 Mantenimiento de Software

a. La documentación de todos los cambios hechos al software se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software, éste deberá firmar un acuerdo de no divulgación y utilización no autorizada del mismo.
b. El área de desarrollo de sistemas no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. A su vez, se contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

5.3 Control de Datos

5.3.1 Disposiciones generales de uso de datos Cruz Roja Costarricense

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. Para identificar la naturaleza de la información, los colaboradores deben de utilizar prefijos como indicadores generales los cuales deben ser: Financiero, Administrativo, Legal, TI, Talento Humano, etc. Todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.
c. Las jefaturas de los departamentos son las encargadas de brindar acceso de la información a terceras personas.
d. 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.
e. La responsabilidad para definir la clasificación de la información debe ser tanto del dueño de la información como del área encargada de la seguridad informática**.**
f. El departamento de TI, mediante un software deberá de controlar el acceso de medios extraíbles (USB, discos duros externos) para evitar la fuga de la información institucional.
g. Si en el ejercicio de sus funciones la auditoria, fiscalía general y departamento de procesos disciplinarios requiere acceso a la información confidencial de los colaboradores, deberán de presentar la solicitud por escrito sobre la información especifica que desean conocer; esta solicitud será analizada por el departamento de TI considerando la ley de Protección de Datos Personales.

5.3.2 Almacenamiento masivo y respaldo de la información

a. Toda información sensible y confidencial debe estar encriptada (tener clave), en cualquier medio de almacenamiento, transporte o transmisión.
b. Toda información sensible debe tener un proceso periódico de respaldo, la fecha de la última modificación y la fecha en que deja de ser sensible.
c. Todos los medios físicos (computadoras, servidor físico o medio de Backup corporativo) o en la nube donde la información de valor, sensitiva y crítica sea almacenada por períodos mayores a seis meses, no deben estar sujetos a un rápido deterioro.
d. Los respaldos de información de valor o sensible debe tener un proceso periódico de validación con el departamento de TI en conjunto con la jefatura o director de área para ser almacenados en un medio en la nube o local (computadoras, servidor físico o medio de Backup corporativo) con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.
e. Toda la información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas y leyes vigentes por el Gobierno de Costa Rica.
f. Si se da un despido o bien el colaborador se va de Cruz Roja Costarricense, el Departamento de TI respaldará aquella información que pertenezca a la institución y sea estrictamente de carácter laboral. Este proceso se realizará en conjunto con el Departamento de Talento Humano como testigo del proceso y el colaborador le indicará a TI si tiene alguna información personal para que proceda a realizar el respaldo esta, recordándole que no se puede llevar ninguna información laboral según lo indicado según el PGA-TH-02 Desvinculaciones del personal de CRC.
g. Los 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 el colaborador podrá ser susceptible a un proceso sancionatorio.

5.3.3 Almacenamiento en forma impresa o documentos en papel

a. Para todos los mensajes remitidos en formato libre de texto que contengan información sensible para el negocio debe numerarse cada línea y los documentos oficiales de la entidad deben de ir con su sello y número especifico.
b. Todas las copias de documentos sensibles deben ser numeradas individualmente con un número secuencial para que las personas responsables puedan localizar rápidamente los documentos e identificar algún faltante de la misma.
c. Si es algún documento sensible en forma físico cada responsable debe de triturarlo y asegurarse que no sea leído de ninguna manera.

5.3.4 Administración de la información

a. 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.
b. 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.
c. 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.
d. Los colaboradores no deben destruir, copiar o distribuir los archivos de Cruz Roja Costarricense sin los permisos respetivos de las jefaturas directas.
e. Es responsabilidad del 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.
f. Los cruzrojistas deben bloquear sin excepción alguna su computadora si se levantan de su escritorio.
g. Los cruzrojistas con firma digital deben de disponer de todos los drivers para el correcto funcionamiento de esta.
h. El formato único para firmar de forma digital es el pdf con la aplicación firmador libre o bien el sistema Gaudí (sistema para firmar digitalmente) emitido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
i. Será responsabilidad de los cruzrojistas verificar que todos los documentos internos y externos que estén firmados digitalmente cumplan con integridad, autenticidad y sellado en el tiempo, lo anterior para garantizar la validez jurídica según lo indicado en la Ley 8454 de certificados, firmas digitales y documentos electrónicos.
j. Si los Cruzrojistas por sus funciones necesitan sacar información impresa de las sedes de la Cruz Roja esta debe de ser bajo autorización de su jefatura directa.

5.3.5 Manejo de Base de Datos Institucionales

a. Todo acceso a las bases de datos de Cruz Roja debe contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
b. El Departamento de TI velará porque toda base de datos que sea instalada cuente con los controles de seguridad que garanticen la confiabilidad de la información.
c. Las jefaturas departamentales deberán solicitar formalmente el acceso a la información de las bases de datos para los funcionarios a su cargo, indicando el nivel de acceso con el que ingresarán a los sistemas.
d. El Departamento de Tecnologías de Información establecerá 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.
e. Las dependencias “dueñas” de la información, deberán participar junto con el Departamento de Tecnologías de Información, para verificar si la información de los respaldos o la restauración de la base de datos fue exitosa.
f. Las Bases de Datos Institucionales deben de estar debidamente inscritas a la agencia de protección de datos de los habitantes y cumplir la Ley de Protección de Datos y su reglamento.
g. Toda migración de base de datos deberá ser realizada por el encargado de las bases de datos del Departamento de Tecnologías de información o personal externo que corresponda bajo la supervisión del Departamento de Tecnologías de información.

h. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.
i. Se debe de documentar en la bitácora todo cambio realizado a nivel de base de datos.

5.3.6 Acceso a la información por parte de terceros y a 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.

5.3.7 Documentación Departamento de Tecnologías de la Información

a. El Departamento de Tecnologías de la Información debe documentar formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.
b. El Departamento de Tecnologías de la Información mantendrá un archivo de gestión de documentos, debidamente ordenado y clasificado para el registro y custodia de la documentación administrativa y de actividades técnicas que desarrolla; y mantendrá como mínimo dentro de sus archivos de gestión, las siguientes documentaciones:
    - Documentación sobre solicitudes de servicio recibidas.
    - Documentación de inventario de equipos de cómputo, periféricos y de telecomunicaciones.
    - Documentación de inventario de software instalado en equipos.
    - Documentación del mantenimiento correctivo de equipos de cómputo, periféricos y telecomunicaciones.
    - Documentación de licencias de software adquiridas.
    - Documentación de proyectos formalmente desarrollados.
    - Documentación administrativa de los funcionarios del Departamento.
    - Políticas Seguridad de la Información Normas Generales de Tecnologías de la Información.
    - Manual de procedimientos y puestos de Tecnologías de la Información.

5.4 Control de Hardware

a. Los activos tecnológicos adquiridos por fondos públicos o propios que pertenezcan a las sedes del Gran Área Metropolitana, los Centros Regionales y los Comités Auxiliares ubicados en todo el territorio nacional, podrán disponerse fuera de las instalaciones de Cruz Roja previo cumplimiento y verificación de los siguientes requisitos autorizados por el Departamento de TI:
    - Cada colaborador (a) deberá llenar la boleta de retiro de equipo tecnológico, la cual deberá ser firmada por el departamento de Tecnologías de Información.
    - Para los casos de disposición de equipo tecnológico fuera de los Comités, cada colaborador (a) deberá llenar la boleta de salida de activos la cual deberá ser firmada y almacenada en un archivo por el administrador (a) del Comité.
b. Es responsabilidad de cada colaborador no consumir alimentos ni ingerir líquidos en el espacio donde este desarrollando su trabajo con el equipo de cómputo operando.
c. Se debe de mantener el espacio físico donde opera el equipo de cómputo limpio y sin humedad alguna.
d. Los cruzrojistas deberán de 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. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Departamento de TI para que se proceda a su revisión.
e. Los cruzrojistas deberán de desconectar el fluido eléctrico de computadoras, mouse inalámbrico y algún otro periférico que este a su cargo en periodos de fines de semana, semana santa, navidad, vacaciones o algún otro acontecimiento que dura más de tres días esto como medida de seguridad y no sobre carga los equipos tecnológicos.
f. Los cruzrojistas deberán de respaldar la información que consideren sensible y mantener esta en la nube si es necesario, esto para evitar alguna pérdida de información de algún proceso de reparación que realice el departamento de TI.

g. Queda totalmente prohibido que los cruzrojistas reparen o desarmen algún equipo computacional, de tener alguna complicación es importante que siempre lo reporten al departamento de TI.
h. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Departamento de TI, que tendrá que velar por su uso y cuidado.
i. El departamento de TI debe de asegurar en su infraestructura tecnológica aplicar y llevar un control de gestión de cambios realizados en los sistemas así mismo como la infraestructura tecnológica.
j. En caso de robo, de los equipos tecnológicos asignados, deberá reportarlo inmediatamente al departamento de TI y este gestionará con la administración el procedimiento a seguir.
k. Es responsabilidad del Departamento de TI hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue.
l. Es responsabilidad del Departamento de TI valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.
m. Los cruzrojistas tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.
n. Las ampliaciones, modificaciones o adquisición de equipo de cómputo, así como la actualización y compra de software, se harán únicamente con el aval por colaboradores del Departamento de TI.
o. El Departamento de Tecnologías de Información determinará cuál es el antivirus oficial y lo instalará en los equipos institucionales, cuando se cuente con la debida licencia. Asesorará a la Administración para que gestione la compra de las licencias requeridas.
p. El Departamento de Tecnologías de Información será la responsable de documentar y aplicar procedimientos para nombrar los equipos. Se utilizará un nombre en letra mayúscula compuesto así: CRC-DEPARTAMENTO-001. Por ejemplo: CRC-PROVEEDURIA-001.
q. Los cruzrojistas deben reportar al Departamento de Tecnologías de Información cuando se le asigna una PC. Para ello utilizarán la Boleta de Traslado de Equipo, diseñada por el Departamento de TI o cualquier otro medio documental establecido para indicar un traslado de equipo. El mismo medio documental será usado por la persona funcionaria para notificar al Departamento de Tecnologías de Información si un equipo a su nombre fue reasignado a otro empleado. Esto con el fin de que el Departamento de Tecnologías de Información pueda renombrar los equipos acordes a la persona responsable del activo y mantener actualizado el registro y estatus de los equipos institucionales y notificarlo al área de activos fijos institucionales.

5.4.1 Adquisición de nuevas tecnologías

a. Todos los procesos institucionales de adquisición de recursos informáticos y tecnológicos deben ser valorados y previamente aprobados por el departamento de Tecnologías de la Información el cual define las especificaciones técnicas para la adquisición mediante fondos propios o públicos, donación, venta, reubicación, préstamo, cesión, remate o por cualquier medio del hardware.
b. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política del Departamento de TI recomendar aquellos que ofrezcan calidad comprobada, SLA (Service Level Agreement) ágil, mantenimiento y sean referentes en el mercado nacional.
c. Para el trámite de adquisición de nuevos recursos informáticos, el Departamento de TI asesorará a la Proveeduría Institucional en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
d. La Proveeduría en conjunto con el departamento de Tecnologías de Información procederán con la compra de nuevas tecnologías mediante los procedimientos de adquisición de bienes y servicios establecidos en el reglamento de compras interno de la Cruz Roja, principios de la ley de contratación administrativa, la ley de Contratación administrativa y su reglamento y la ley de compra Pública, o bien, la normativa que se encuentre vigente al momento de aplicación de esta política.
e. El Departamento de TI y la Proveeduría Institucional velará porque los recursos informáticos adquiridos sean enviados y utilizados por la misma dirección en que surgió la necesidad de compra.
f. El Departamento de TI deberá revisar el inventario del equipo por lo menos una vez al año, realizando los cambios que sean necesarios. Hará un informe a la Administración sobre las diferencias y/o deficiencias encontradas.
g. El Departamento de TI tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales.

5.4.2 Manejo de desechos de los medios tecnológicos

a. Los equipos electrónicos para desechar serán revisados por funcionarios del Departamento de TI, generando un acta de desecho la cual será entregada a la Unidad de activos fijos como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.
b. Cruz Roja Costarricense procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente.

5.5 Control de redes

a. El Departamento de TI será la dependencia responsable de la administración y uso de la red interna de datos.
b. El Departamento de TI garantizará el acceso controlado en la red interna de Cruz Roja Costarricense.
c. El Departamento de TI monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.
d. No es permitido a ningún colaborador, excepto al departamento de TI manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
e. El Departamento de TI pondrá en funcionamiento herramientas de control que posibiliten detectar, 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.
f. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado. Deberá utilizarse para el cableado de red la certificación vigente en el momento que se instalen nuevas conexiones.
g. Los funcionarios solicitarán asistencia al Departamento de Tecnologías de Información para agregar un equipo a la red institucional.

5.5.1 Uso y acceso a internet, correo electrónico, canales de comunicación internos y periféricos en red

a. Los servicios de Internet y correo electrónico serán administrados por el Departamento de TI.
b. Para la comunicación oficial de Cruz Roja Costarricense debe utilizarse la cuenta de correo institucional, como medio de comunicación oficial para la administración.
c. El correo electrónico institucional es una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información ni de uso para actividades que no sean laborales.
d. El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
e. El Departamento de TI asignará las cuentas de correo de acuerdo con las licencias disponibles.
f. Está prohibido facilitar u ofrecer las cuentas de correo a terceras personas.
g. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
h. Los funcionarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
i. El Departamento de Talento Humano deberá notificar al Departamento de TI cuando se deba crear, cerrar o inhabilitar un usuario de dominio o una cuenta de correo electrónico.
j. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones del Departamento de TI.
k. Se habilita el uso de Whatsapp en los equipos institucionales para los cruzrojistas que sean voluntarios o asalariados como medio de apoyo para el ejercicio de sus funciones; En caso de que el uso inapropiado perjudique los intereses de la Asociación Cruz Roja Costarricense, el infractor será susceptible de un proceso disciplinario y judicial según corresponda.
l. Queda prohibido suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo.
m. Queda prohibido descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional. El Departamento 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.

n. Queda prohibido solicitar los datos de cuentas de correo electrónico de personal activo o inactivo de la institución ya que este acto violenta la privacidad de los datos personales de cada colaborador de Cruz Roja Costarricense.
o. Las herramientas digitales de comunicación interna serán definidas por el por el departamento de Tecnologías de la Información. Queda prohibida la divulgación de información confidencial por este medio.
p. Queda prohibido el acto discriminatorio hacia algún colaborador de Cruz Roja Costarricense por medios digitales.
q. Para enviar, recibir y reenviar mensajes de correo electrónico se aplicarán las siguientes reglas:
    - Se copiarán únicamente en los correos electrónicos a las personas relacionadas con el tema a tratar en el cuerpo del mensaje, esto para evitar saturar el correo de cada colaborador y manteniendo la confidencialidad de la información.
    - En el cuerpo del correo no se permiten colocar ni fondos, ni texturas, esto respetando la imagen gráfica de la institución.
    - Se enviarán mensajes a listas globales de correo electrónico, a menos que la información a trasmitir involucren a toda la Institución se envía al grupo de correo correspondiente.
r. El Cruzrojista que requiere utilizar las impresoras en red disponibles en el edificio Central deberá hacer la solitud respectiva en el Departamento de TI.
s. El Departamento de TI, le asignará una contraseña de acceso a las impresoras a cada funcionario, por lo que queda bajo responsabilidad del Cruzrojista mantener bajo seguridad dicho acceso.
t. Queda prohibido la impresión de archivos personales, ni de terceras personas.
u. El Departamento de TI, mensualmente hará entrega vía correo a las jefaturas Departamentales el informe de impresión de sus funcionarios, para que se tomen las medidas respectivas

5.6 Control de equipos tecnológicos en modalidad teletrabajo

a. La computadora o dispositivos brindados por la institución a los teletrabajadores deberán de contar con una protección de antivirus.
b. Los teletrabajadores cruzrojistas deberán de conectarse a la red institucional únicamente por el VPN instalado por el departamento de TI.
c. Cada teletrabajador cruzrojista, deberá de manejar la mayoría de su información en la red o una infraestructura cloud como office 365 (Microsoft One Drive, Microsoft SharePoint)
d. Los cruzrojistas deberán aplicar medidas preventivas cuando se ausentan de las labores, antes de retirarse del lugar teletrabajable donde se ubique el equipo de cómputo, el colaborador deberá tomar las siguientes precauciones mínimas:
    - 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.
e. El Teletrabajador cruzrojista deberá de contar con el requisito básico de una conexión mínima de internet de 5 Mbps.
f. Si por inconvenientes eléctricos la persona teletrabajadora se queda sin electricidad, esta deberá 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.
g. El teletrabajador cruzrojista deberá de estar de forma “online “y disponible en los horarios respectivos de trabajo según la modalidad de teletrabajo que la institución y su jefatura directa le hayan designado.

5.7 Control de dispositivos móviles

5.7.1 Disposiciones Generales

a. Los dispositivos móviles propios de “La Organización” deben estar inventariados.
b. Los medios de almacenamiento de los dispositivos móviles propios de “La Organización” deben estar cifrados.
c. Deben contar con bloqueo mediante contraseña u otro medio robusto de autenticación.
d. Se debe reportar la pérdida, robo o daño de dispositivos de forma inmediata al conocimiento del hecho.
e. Deben contar con mecanismos de protección ante código malicioso, en caso de que corresponda.
f. Deben tener un sistema operativo obtenido por canales oficiales o instalado de fábrica, así mismo, no deberán ligarse cuentas personales si no únicamente institucionales.
g. Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.
h. 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.
i. Se debe contar con procedimientos para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible allí almacenada.
j. El departamento de Tecnologías de Información será el encargado de reasignación, desconexiones temporales o definitivas, programación o reprogramación de líneas o celulares, cambios de número u otros ante el proveedor de servicios de la línea telefónica celular, previa autorización de la Subgerencia Administrativa.
k. El departamento de Tecnologías de Información previo criterio técnico, será el encargado de recibir la solicitud del interesado, clasificar y emitir el visto bueno según perfil técnico, remitir a la Gerencia dicha solicitud para aprobación, solicitar nuevas líneas y terminales al proveedor, gestionar el contrato de vinculación con la Dirección Jurídica, asignar las líneas y terminales al cruzrojista asimismo, deberá llevar en forma actualizada la lista de usuarios con líneas y terminales propiedad de la Asociación Cruz Roja Costarricense, así como de llevar el inventario actualizado del usuario, líneas telefónica y/o terminal asignado, así como MI-FI¨s institucionales.
l. Tecnologías de Información será el encargado de definir los requerimientos técnicos de acuerdo con los perfiles establecidos por el departamento y le corresponderá custodiar el dispositivo una vez que el funcionario haga entrega de este en caso de terminación de la relación laboral.
m. Los cruzrojistas autorizados para el uso de celulares institucionales son:
    - Órganos superiores: Consejo Nacional, Fiscal general, Fiscales generales adjuntos, y asistentes administrativos, presidente Tribunal de Ética y Disciplina.
    - Gerencia General y subgerentes.
    - Directores Nacional y Jefaturas de Departamentos Nacionales.
    - Presidentes de las juntas directivas regionales y Administradores Regionales.
    - Aquellos usuarios que la subgerencia administrativa designe.
n. Los siguientes perfiles contarán con un límite de consumo, estas líneas cambiarán a modalidad prepago al consumirse el monto disponible para su uso.

    - Perfil Directores- Jefaturas
    - Perfil General- Comités
    - Líneas Sinpe

    Para gestionar la habilitación de las recargas de las líneas prepago, el usuario deberá de solicitar la autorización a la Gerencia, quien previo estudio dará la orden a la unidad fiscalizadora para proceder según corresponde.
o. Queda prohibido a aquellos cruzrojistas a quienes se les ha asignado un servicio de dispositivos móviles y líneas de telecomunicación propiedad de esta Asociación 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.

p. Los cruzrojistas que utilicen los celulares institucionales deberán apegarse estrictamente a las políticas de seguridad de la información y normas generales de T.I. En caso de robo del dispositivo tecnológico, de sus accesorios o de ambos, el cruzrojista responsable del equipo deberá informar al departamento de Tecnologías de información a más tardar el día hábil siguiente para que se proceda a solicitarla suspensión del servicio a la empresa proveedora, así mismo, deberá presentar la respectiva denuncia ante el Organismo de Investigación Judicial (OIJ).

q. 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 el cruzrojista deberá cubrir el costo de la reparación o costo proporcional al monto indicado en los libros de saldos contables, aplicándose la respectiva depreciación.

r. La asignación de dispositivos móviles y líneas de telecomunicación no se considera como parte del salario, por lo que el 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.

s. El 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, deberá hacer la devolución del equipo en presencia de su jefatura inmediata, personeros del departamento de Tecnologías de Información, Talento Humano y la Dirección Jurídica, lo anterior en un plazo máximo de dos días hábiles. Cuando por condiciones de distancia no puedan concurrir los personeros descritos con anterioridad, la entrega del equipo se hará en presencia del administrador del Comité donde labora el usuario del dispositivo móvil, quien verificará mediante acta proveída por el departamento de T.I las condiciones de recibo, y posteriormente, remitirá el dispositivo en un plazo máximo de cinco días hábiles al departamento de Tecnologías de Información ubicado en la sede Central, Zapote. De existir un atraso en la devolución por responsabilidad del cruzrojista a quien se le hubiere asignado el servicio, las multas o demás erogaciones que proceda cancelar al proveedor quedarán bajo su exclusiva responsabilidad.

t. 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 que aprobará la Subgerencia Administrativa con base en los estándares celulares.

u. La subgerencia Administrativa o la jefatura directa del funcionario podrá retirar su uso unilateralmente en cualquier momento y dejar sin efecto la asignación de dispositivos móviles y líneas de telecomunicación –entre otras- por las siguientes causas:
   - Desaparición de la necesidad de esta Asociación, o de las circunstancias que motivaron la asignación del servicio.
   - Cambio de cargo del cruzrojista responsable.
   - Despido del cruzrojista.
   - Limitaciones presupuestarias.
   - Cualquier otro motivo o causa a criterio exclusivo de la Subgerencia Administrativa, donde debe mediar justificación de la naturaleza de esa determinación.

5.8 Gestión de Proyectos Tecnológicos

a. Los usuarios y/o patrocinadores de los proyectos de TI, deben liderar y administrar sus proyectos, con la asesoría e incorporación del Departamento de Tecnologías de Información para coordinarlos siguiendo la metodología de desarrollo de proyectos de TI ya establecida.

b. Todo proyecto en materia de TI deberá ser desarrollado bajo la metodología de Administración y control de los proyectos de TI, utilizada en dicho Departamento.

c. Las jefaturas departamentales no deben adquirir o implementar sistemas, (ya sea por donación, práctica estudiantil, contrato a terceros), sin la debida aprobación del Departamento de Tecnologías de Información.

d. Las dependencias de la Sociedad Nacional deben asesorarse con el Departamento de Tecnologías de Información, para la adquisición de infraestructura, sistemas y asesoría tecnológica.

5.9 Responsabilidades

5.9.1 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.

5.9.2 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.

5.9.3 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.

5.10 Disposiciones Finales

Con la publicación de esta política se deroga toda la normativa interna que refiera a uso de dispositivos tecnológicos en la Sociedad Nacional.