Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja

Seguridad de la información: política de uso aceptable

Número de referencia del documento: 062

Autorización del documento				
Parte interesada	**Nombre**	**Cargo**	**Firma**	**Fecha de aprobación**
Autor	Ed Happ	Jefe, Departamento de Servicios de Información		20.12.2013
Responsable del documento	Michael Veltman	Jefe, Departamento de Recursos Humanos		19.02.2014
Aprobación del documento	Malika Ait-Mohamed Parent	Subsecretaria general, División de Servicios a Órganos de Gobierno y de Gestión		20.12.2013
Aprobación del documento	Matthias Schmale	Subsecretario general, División de Desarrollo de Conocimientos y de las Sociedades Nacionales		20.12.2013
Otras partes interesadas	Sayed Hashem	Jefe, Departamento de Auditoría y Gestión del Riesgo		20.12.2013
Otras partes interesadas	Elise Baudot	Jefa, Departamento de Asuntos Jurídicos		20.12.2013

Número de versión: 2.5
Fecha de autorización: 19.02.2014
Clasificación del documento: interno

Control del documento

El presente documento está sujeto a modificaciones controladas y toda enmienda de las versiones principales se indicará en el cuadro que figura a continuación.

Historial de modificaciones

Versión	Fecha	Notas
1.0	Octubre de 2007	Primera versión de la política
2.1	7 de junio de 2013	Política revisada
2.2	17 de junio de 2013	Proyecto revisado donde se incorporaron observaciones recibidas al 14 de junio de 2013, de las partes interesadas en el proyecto.
2.3	2 de julio de 2013	Proyecto revisado donde se incorporaron observaciones recibidas al 1 de julio de 2013, de las partes interesadas en el proyecto.
2.4	15 de julio de 2013	Proyecto revisado donde se incorporaron observaciones recibidas al 12 de julio de 2013.
2.5	29 de julio de 2013	Proyecto revisado donde se incorporaron observaciones recibidas al 26 de julio de 2013.

Versiones

Los usuarios del presente documento deben ser conscientes de que el ejemplar impreso tal vez no corresponda a la versión más actual existente. La última versión, que sustituye a todas las anteriores, está disponible en FedNet.

Glosario

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[1] para acceder a la información que necesite en una ubicación específica y en el formato adecuado.

Empleado: este término hace referencia a un subgrupo del personal de la Federación Internacional. Incluye a miembros del personal adscritos a la oficina central, en Ginebra, y a los delegados (véase el Reglamento de Personal y el Reglamento Interno de Personal de la Federación Internacional).

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 Federación Internacional se deberán eliminar con arreglo al calendario aprobado de retención y eliminación de registros del departamento correspondiente (véase más detalles bajo las secciones de la plataforma FedNet relativas a categorías de archivos e instrucciones para la retención y la eliminación de estos en la Federación Internacional).

Personal: las expresiones personal y miembros del personal hacen referencia a los empleados de la Federación Internacional (miembros del personal adscritos a la oficina central, en Ginebra, y delegados), el personal local, los consultores, los voluntarios y los pasantes, así como al personal en comisión de servicios y a todas las personas que realizan actividades en nombre de la Federación Internacional y amparados por la personalidad jurídica de esta (véase el Código de Conducta de la Federación Internacional).

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

[1] 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.

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 Federación Internacional, los contratistas y los terceros proveedores que gocen de autorización para acceder, tratar o utilizar la información o los datos de la Federación Internacional.

Índice

1. Introducción

La Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (Federación Internacional) confiere distintos usos y destinos a la información que recibe y procesa. La reputación de la Federación Internacional, 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[2], los contratistas y los terceros proveedores que gocen de autorización para acceder, tratar o utilizar la información o los datos de la Federación Internacional) incumplan las normas y los controles adecuados en lo que atañe a la gestión de la seguridad de la información.

Incumbe al Departamento de Servicios de Información de la Federación Internacional preservar la seguridad y la integridad de los sistemas de información y comunicaciones de la organización. Junto con el Departamento de Recursos Humanos, vela por que los usuarios conozcan el marco de seguridad de la información[3] establecido por la Federación Internacional 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[4]. El Departamento de Servicios de Información también es responsable de velar por que se adopten las medidas necesarias si no se cumplen esas normas.

2. Objetivo

Con arreglo al marco de seguridad de la información establecido por la Federación Internacional, la presente política define las obligaciones y limitaciones de los usuarios en las siguientes actividades:

- aplicación de los controles adecuados para preservar la seguridad de la información, y
- utilización de 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).

3. Ámbito de aplicación y alcance

El marco de seguridad de la información, con inclusión de la presente política, se aplica a todos los usuarios. La aplicación de esta última también concierne a las Sociedades Nacionales participantes y a las Sociedades Nacionales anfitrionas que hayan firmado un acuerdo con la Federación Internacional 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. Las Sociedades Nacionales que no estén integradas en las delegaciones de la Federación Internacional sobre el terreno no estarán sujetas a la presente política de uso aceptable y gozarán de acceso a la red exclusivamente en calidad de visitantes, a menos que suscriban la política.

La política será de aplicación obligatoria con respecto a los activos de información y datos en cualquier formato con inclusión, 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 informáticos, soporte lógico de procedimientos y de apoyo, y dispositivos de almacenamiento de datos.

---

2 Véase en el glosario la definición de “personal”.

3 Véase más detalles en la Carta sobre la seguridad de la información.

4 A los efectos de esta política, los recursos de las tecnologías de la información y las comunicaciones incluirán equipos informáticos, como ordenadores de escritorio y portátiles de todo tamaño, teléfonos móviles y con conexión vía satélite, y todo tipo de aplicaciones, datos y programas informáticos conexos utilizados por la Federación Internacional bajo licencia o en propiedad.

4. Requisitos para la seguridad de la información

Incumbe a todos los usuarios la responsabilidad de aplicar los controles apropiados con objeto 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 en la responsabilidad de la Federación Internacional[5].

Según se establece en las Normas de clasificación de la información[6], los controles adecuados se definen con arreglo a la categoría de la información o de los datos que se estén utilizando, que será especificada por el propietario del activo de información[7] en el propio activo de información o dato, independientemente de su formato (impreso, electrónico)[8].

5. Prácticas recomendadas

Los usuarios deberán seguir las normas 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. 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 Servicios de Información no establece copias de seguridad de la unidad local ni del escritorio del ordenador.
- Cuando se contrate a personal temporero u ocasional, se deberá determinar los sistemas y carpetas de datos a los que necesitarán tener acceso esos usuarios para cumplir con sus obligaciones antes de solicitar al servicio de asistencia a los usuarios que se configure el acceso a la red.
- Los usuarios deberán bloquear los ordenadores antes de dejarlos desatendidos durante períodos breves y finalizar la sesión en caso de ausencia prolongada.

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

El uso de los recursos y tecnologías de la información y las comunicaciones de la Federación Internacional se concede con arreglo a los principios que se exponen a continuación.

1. Se podrá utilizar los recursos y las tecnologías de la información y las comunicaciones solamente con fines legítimos que tengan relación con las actividades de la Federación Internacional. 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 del cargo.

2. Los recursos y tecnologías de la información y las comunicaciones se utilizarán con arreglo a los principios fundamentales del Movimiento, a la presente política y al Código de conducta del personal.

---

5 Véase Carta sobre la seguridad de la información para más detalles sobre las funciones y las responsabilidades,

6 Véase las Normas de clasificación de la información en la plataforma FedNet. Los controles de clasificación de la información también figuran en el anexo del presente documento.

7 Véase en el glosario la definición de "propietario de activo de información".

8 Véase las Normas de clasificación de la información.

3. Los usuarios serán responsables del cuidado de los equipos de tecnologías de la información y las comunicaciones que hayan recibido (como ordenadores portátiles o teléfonos móviles). La pérdida de cualquier equipo deberá comunicarse cuanto antes al servicio de asistencia a los usuarios del Departamento de Servicios de Información, aportando detalles sobre los datos almacenados en él.

4. El empleo de los recursos y las tecnologías de la información y las comunicaciones deberá respetar todas las leyes nacionales e internacionales aplicables relativas 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 concesión de licencias.

5. 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.

7. 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 personal o las políticas de recursos humanos. A continuación figuran ejemplos de actividades que son inaceptables y están prohibidas.

1. El empleo de los recursos y las tecnologías de la información y las comunicaciones de la Federación Internacional de manera que no guarde consonancia con el Código de Conducta o de la presente política.

2. La descarga, el envío de mensajes de correo electrónico, 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 sumaria.

3. Todo intento para superar o desactivar las medidas de seguridad, acceder a datos o modificarlos sin contar con la autorización debida.

4. El empleo de recursos y las tecnologías de la información y las comunicaciones con una identidad ficticia o perteneciente a otra persona (a menos que sea necesario para el ejercicio de las funciones oficiales, por ejemplo, para comprobar los sistemas informáticos).

5. El uso o la instalación de dispositivos no normalizados o de programas informáticos no tolerados[9]. Todo uso de los sistemas de información deberá ser conforme a las obligaciones contractuales de la Federación Internacional, con inclusión de las limitaciones definidas en los programas informáticos y otros contratos de concesión de licencias.

6. Los usuarios no configurarán reglas en Outlook para el reenvío de correo electrónico a sus direcciones personales ni a ninguna otra dirección ajena a la Federación Internacional. Con ello se reduce el riesgo de que el material de carácter reservado sea reenviado a sistemas de correo electrónico cuya seguridad sea inadecuada.

[9] Véase la lista de verificación de excepciones para el sistema de tecnologías de la información en https://servicedesk.ifrc.org.

7. 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 de que esto incluye el incumplimiento de las leyes de derechos de autor, que rigen la copia, la visualización y el uso de programas informáticos y demás obras en formato digital.

8. Uso personal

La Federación Internacional permite a los usuarios un uso personal razonable y limitado de los recursos informáticos. Corresponde exclusivamente a la Federación Internacional la responsabilidad de determinar qué uso es "razonable", teniendo en cuenta las circunstancias pertinentes. La Federación Internacional 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 Federación Internacional. 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 Federación Internacional (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 Servicios de Información.

Aunque la Federación Internacional 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 Federación Internacional no puede garantizar el carácter confidencial de esos archivos o mensajes, y podrá limitar o poner fin a esas actividades cuando lo considere necesario.

9. Uso del correo electrónico

Los usuarios deben ser conscientes de que, cuando envían un mensaje de correo electrónico desde una dirección "___.ifrc.org", lo hacen en representación de la Federación Internacional. Los mensajes electrónicos pueden ser jurídicamente vinculantes para la Federación Internacional 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 (lo que en inglés se denomina *flaming*), enviar correo basura o mensajes en cadena, suplantar la identidad de otro usuario y 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 Federación Internacional y deberán conservarse durante el tiempo que sea necesario conforme a los requisitos administrativos y jurídicos de la Federación Internacional.

10. 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 Federación Internacional son propiedad de la organización. La Federación Internacional 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, y
- verificar los dispositivos extraíbles para comprobar que no tienen virus antes de usarlos en los equipos de la Federación Internacional.

11. Derechos de autor, licencias y programas informáticos

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

Los usuarios que deseen instalar programas informáticos en su ordenador deberán seguir las políticas y los procedimientos correspondientes de la Federación Internacional, que pueden solicitar al Departamento de Servicios de Información.

12. Cumplimiento de normas y procesos

La Federación Internacional 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 Federación Internacional 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, las normas o las políticas de la Federación Internacional, 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 Federación Internacional.

El acceso a la información sin el conocimiento o el consentimiento de los usuarios debe ser aprobado por los responsables del Departamento de Servicios de Información y el Departamento de Recursos Humanos (o sus delegados), excepto cuando sean los responsables de la gestión quienes lo exijan, para preservar la integridad de las instalaciones. Además de acceder a los sistemas informáticos, la Federación Internacional podrá eliminar o limitar los privilegios de acceso de un usuario a los recursos de las tecnologías de la información y las comunicaciones.

Sanciones

Los usuarios tendrán que rendir cuentas por todo incumplimiento de la presente política. La inobservancia de esta u otras políticas, normas, procedimientos y reglamentos conexos darán lugar a medidas disciplinarias con arreglo al capítulo IX del Reglamento Interno de Personal o de los reglamentos de personal locales, según corresponda. Si un contratista contraviene las políticas, normas, procedimientos o reglamentos de la Federación Internacional, esta podrá rescindir el contrato. Además, la Federación Internacional 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).

Política de uso aceptable, Federación Internacional, diciembre de 2013.

DECLARACIÓN DE CONFORMIDAD

Declaro que he recibido, he leído y he comprendido el documento "Seguridad de la información: política de uso aceptable" de la Federación Internacional. Comprendo que esta política forma parte de las condiciones de empleo y servicio en la Federación Internacional y me comprometo a acatarla.

Firma _____

Nombre _____

Lugar _____

Fecha _____

Anexo: Controles de clasificación de la información[10]

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[11].

Categoría: muy reservada

VIDA ÚTIL DE LA INFORMACIÓN		Controles de información "MUY RESERVADA"
Uso y modificación	Cambio de formato	No se debe duplicar la 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 modificables).
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 recibo firmado.
	Transmisión electrónica de los datos	✓ Todas las transmisiones de datos se realizarán mediante una aplicación de mensajería autentificada 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 reenviarlos a otros destinatarios. ✓ Se solicitará acuse de recibo 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 debe mantenerlas 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 salir de la sala.
	Copia	✓ Se debe realizar el 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.

[10] Véase las Normas de clasificación de la información en la plataforma FedNet para consultar más detalles.
[11] Véase los procedimientos, normas y directrices de tecnologías de la información en la plataforma FedNet para consultar más detalles.

VIDA ÚTIL DE LA INFORMACIÓN		Controles de información "MUY RESERVADA"
		✓ 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, un dispositivo USB 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 Federación Internacional no tenga control sobre ellos y a las que pueda acceder el gobierno (por ejemplo, Dropbox o 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 período de retención[12]. ✓ Los documentos definitivos y de trabajo conexos que se deba transferir a los archivos de la Federación Internacional para almacenamiento al culminar el período de retención deberán ser remitidos 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 deberá imprimir los documentos electrónicos que se deba transferir a los archivos de la Federación Internacional 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.

[12] Véase en el glosario la definición de "período de retención".

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, 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 Federación Internacional (por ejemplo, entre las oficinas sobre el terreno y Ginebra).
	Transmisión electrónica de los datos	✓ La transmisión electrónica de 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 recibo electrónico.
	Conversaciones orales	✓ Se debe mantenerlas 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 reservado 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 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 o más rigurosas. ✓ La información reservada se podrá almacenar fuera de

VIDA ÚTIL DE LA INFORMACIÓN		Controles de información "RESERVADA"
		los locales de la Federación Internacional, siempre y cuando se apliquen los 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 oficial 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 Federación Internacional 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 deba transferir a los archivos de la Federación Internacional 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, direcciones que acaben en @ifrc.org) la primera vez que se distribuya la información interna[13]. ✓ Sin limitaciones para la impresión o el envío por facsímil.

[13] Las Sociedades Nacionales participantes o las Sociedades Nacionales anfitrionas integradas en una delegación de la Federación Internacional serán responsables de la distribución posterior de la información interna pertinente.

	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 las 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 Federación Internacional 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 físicamente o se reformatearán cuando culmine el período de retención. Se deberá imprimir los documentos electrónicos que se deba transferir a los archivos de la Federación Internacional 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: 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 Federación Internacional 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 deba transferir a los archivos de la Federación Internacional 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.