Versión/Clasificación:	1.0 / Interno		
Autor:	Jayesh Patel (Seguridad TI)		
Revisado por:	Chet Kuchinad (CPO-HR), Khaleel Desai (Consejero Legal), Graham Kent (Servicios Compartidos de TI), Nigel Gavin (Gobernanza Financiera)		
Aprobado por:	Jon Watts (CFO)		
Fecha de aprobación:	21/12/2016	Próxima fecha de revisión:	20/12/2017

POLÍTICA PARA EL USO ACEPTABLE DE LAS TI

PANORAMA

Este documento describe instrucciones sobre el modo en que Save the Children International (SCI) requiere que su personal, personal contratado y cualquier tercero actúe al usar información de SCI y los activos de TI que apoyan nuestra misión para alcanzar hasta el último niño o niña. Esta política será considerada como parte integrante del Código de Conducta de SCI. Debe ser leída junto con la Política de Seguridad de TI de SCI y la Política de Protección Infantil de SCI.

El incumplimiento para seguir esta política podría ponerlo en riesgo a usted, sus colegas, niños y niñas con quienes trabajamos o a nuestros donantes, lo que ocasionaría un impacto y perjuicio para la reputación de nuestra organización.

El uso indebido e intencional o el incumplimiento para seguir esta política será tomada muy seriamente por la organización y podría conllevar acciones disciplinarias. En algunos países y jurisdicciones, SCI podría estar obligada a notificar a las agencias de orden interno ante cualquier infracción y los usuarios podría ser acusados y procesados.

En este documento, se incluyen ejemplos de acciones y actividades que son consideradas faltas. Estos ejemplos no constituyen una lista exhaustiva, pero están diseñados para ayudarle a comprender los requerimientos y cómo se aplican en su caso. Usted debe reportar cualquier falta o falta potencial a esta política que usted conozca, tanto si se relacionan con usted, sus reportes directos u otros. Si no tiene certezas, debe solicitar consejo sobre las medidas adecuadas a su gerente de línea o enviando un correo electrónico a 'itsecurity@savethechildren.org'.

ALCANCE Y APLICACIÓN

Esta política se aplica a todo el personal de SCI y de los miembros, incluyendo contratistas, personal temporal, socios, consejeros, voluntarios y otros que trabajen por parte de SCI y/o usen información de SCI (electrónicamente o impresa) y sistemas de TI para negocios o uso personal.

Esto incluye, pero no se limita al uso Seguro del correo electrónico, Internet, telefonía, herramientas de comunicación instantánea, impresiones, faxes, así como cualquier software provisto por SCI, aplicaciones y hardware, incluyendo computadoras, laptops, celulares o teléfonos Smart y tabletas.

En cualquier ocasión en que parte o partes de esta política entren en conflicto con cualquier requerimiento legal local, las leyes o normativas locales deben prevalecer, siempre que no generen obligaciones adicionales, mayores o más onerosas. Sin embargo, esta política se aplicará total o parcialmente cuando no exista conflicto con las leyes locales.

CUMPLIMIENTO

Medición

Esta política para el Uso Aceptable de TI respalda el Código de Conducta de SCI y la Política de Seguridad de TI. Es un documento obligatorio aplicable a todo el personal y el cumplimiento será medido mediante la aceptación formal del personal y su recertificación anual, según se aplique.

Excepción

Esta política debe ser acatada por todo el personal de SCI en todo momento, excepto si se notifica expresamente a 'itsecurity@savethechildren.org' o al Jefe de Seguridad de TI sobre cualquier excepción que surja al cumplir con la normativa local, cuando sea adecuado.

CONTENIDO

Esta política para el Uso Aceptable de TI especifica 8 requerimientos clave:

1. Comprender nuestra información y niveles de clasificación
2. Comprender cómo proteger la información adecuadamente
3. Usar los sistemas de TI, correo electrónico e internet de SCI adecuadamente
4. Mantener seguros sus IDs de usuario y contraseñas
5. Usar las redes sociales apropiadamente
6. Gestionar cuidadosamente los riesgos a los sistemas de TI por el phishing, correos basura y virus
7. Reportar incidentes de Seguridad de TI y de Protección Infantil inmediatamente
8. Usar computadoras y teléfonos celulares provistos por SCI de manera segura y adecuada

Cada uno de estos requerimientos ha sido descrito en detalle en la siguiente sección.

Versión/Clasificación:	1.0 / Interno		
Autor:	Jayesh Patel (Seguridad TI)		
Revisado por:	Chet Kuchinad (CPO-HR), Khaleel Desai (Consejero Legal), Graham Kent (Servicios Compartidos de TI), Nigel Gavin (Gobernanza Financiera)		
Aprobado por:	Jon Watts (CFO)		
Fecha de aprobación:	21/12/2016	Próxima fecha de revisión:	20/12/2017

REQUERIMIENTOS PARA EL USO ACEPTABLE DE TI

1. Comprender nuestra información y niveles de clasificación

Los dueños y usuarios de la información en SCI deben utilizar la siguiente matriz, hecha para fines de orientación, para clasificar los activos de información procesados usando los sistemas de TI y para la necesidad de protección.

Nivel de clasificación	Definición/Impacto	Ejemplos
Sensible (Nivel IV)	Estrictamente destinados para uso interno de SCI y/u miembros. La divulgación podría generar un impacto grave y negativo para SCI, los niños y niñas por quienes trabajamos, nuestros donantes y/o socios corporativos, lo que llevaría a repercusiones financieras, así como una opinión pública contraria.	• Información de niños y niñas vulnerables, incluyendo datos personales o información médica • Información de RRHH (información del empleado) • Información individual del donante, incluyendo datos bancarios o de tarjetas de crédito • Cualquier consejo o comunicación con abogados internos o externos • Cualquier información vinculada a investigaciones por fraude • Información relacionada con alegatos de Protección Infantil, incluyendo datos de las víctimas, testigos o delincuentes
Confidencial (Nivel III)	Destinado al uso interno de SCI y/u miembros. La divulgación podría tener un impacto negativo en SCI,	• Información de desempeño del empleado • Detalles de configuración de TI • Informes de auditoría interna/externa • Información de proyectos/programas globales

	nuestros colaboradores y los programas mundiales que dirigimos.	• Informes presentados al Directorio de SCI • Informe financiero de fin de año sin publicar • Documentos de estrategia relacionados con ingresos, donantes institucionales o estructura de costos • Planes y métodos de seguridad (no TI) • Capital intelectual de SCI, que consta de la experiencia colectiva, conocimientos, habilidades e información para dirigir los Programas Internacionales
Interno (Nivel II)	Esta clasificación se aplica a todo el resto de la información, de la que no se espera un impacto grave o negativo para SCI o nuestros empleados, grupos de interés, programas globales o socios comerciales. Sin embargo, esta información es importante para dirigir nuestras actividades y negocios.	• Correos electrónicos y directorio telefónico de SCI • Comunicaciones de toda la organización • Programas y materiales de capacitación internos/externos • Información de reuniones • Documentos de políticas y orientación • Otra información financiera a discreción del usuario, por ejemplo, información de tesorería, de gastos, etc.
Público (Nivel I)	Esta clasificación se aplica a información	• Información publicada en https://www.savethechildren.net,

	que ha sido aprobada explícitamente por un miembro autorizado o por el SLT de SCI para ser comunicada al público. Es poco probable que este tipo de información ocasione un impacto en SCI.	• Volantes y folletos de servicios • Anuncios de programa • Vacantes y anuncios de trabajo • Notas de prensa por parte del personal autorizado

Nota

- Los dueños de la información tienen la responsabilidad principal de asegurarse de que la información de SCI esté adecuadamente clasificada en línea con las pautas antes mencionadas.
- La clasificación aplicada debe ser claramente visible en documentos electrónicos o de formato físico.
- Es una buena idea incluir la clasificación del documento en la primera página o a pie de página si la información es almacenada en formato electrónico.

2. Comprender cómo proteger la información adecuadamente

Al trabajar con **cualquier información de SCI** usted debe:

- Evitar dejar su laptop y teléfonos inteligentes desatendidos.
- Siempre activar una contraseña o codificación de pin fuertes en las laptops o teléfonos inteligentes que usen para trabajar.
- Activar el bloqueo de pantalla en sus laptops o computadoras cuando dejen su escritorio en la oficina o cuando trabajen desde casa.
- Asegure la integridad física de su laptop, teléfono celular o dispositivo de almacenaje en todo momento, incluso en lugares como salones en los aeropuertos, oficinas de campo y otros lugares apartados.

Al trabajar con **información interna de SCI** usted debe:

- Compartirla solo con destinatarios autorizados, incluso colegas de SCI y terceros según sea necesario.
- Asegurarse de que ha incluido a los destinatarios correctos de un correo electrónico antes de darle 'ENVIAR'.
- Siempre utilice servicios de correo electrónico y mensajería de SCI autorizada y segura (Skype Empresarial) para trabajar. NO use servicios web (p.e. Gmail, Hotmail o Skype) para realizar su trabajo y sus obligaciones.

- Si está en teleconferencia, siempre identifique a los participantes en la llamada antes de compartir información.
- Tome las precauciones debidas al discutir el trabajo o planes de trabajo en el teléfono en zonas públicas donde pueda ser escuchado.

Al trabajar con **información confidencial o sensible de SCI,** usted debe seguir los requerimientos internos de SCI y además:

- Estar autorizado para manejarla.
- Si está en copias impresas, CUSTODIARLA en un gabinete seguro si se deja desatendida.
- CODIFICARLA al enviarla a otros destinatarios autorizados fuera de SCI por correo electrónico o almacenándola en un medio portátil como HDD, CD, DVD, memoria USB. Contactar a su soporte de TI, Equipo de RISC o escribir a 'itsecurity@savethechildren.org' para mayor orientación sobre los requerimientos y métodos de codificación.
- Si la información es física o impresa, desecharla de manera segura: cortarla en tiras o en una papelera confidencial.

Nota

- Recuerde aplicar los controles de seguridad de TI adecuados al manejar diferentes tipos de información. Si tiene dudas, contacte a su soporte de TI para mayor orientación.
- La información clasificada sensible o confidencial de SCI no debe ser enviada por correo electrónico a ninguna cuenta de correo personal (p.e. Gmail, Yahoo, Hotmail, etc.) ni copiada en ningún dispositivo personal (p.e. laptops, computadoras, teléfonos inteligentes) que no haya sido proporcionado por SCI o que no cumpla con los requerimientos de traer su propio equipo (BYOD - Bring Your Own Device) de SCI.

3. Usar los sistemas de TI, correo electrónico e internet de SCI apropiadamente

NUNCA USE sistemas de TI de SCI para lo siguiente:

- Transmitir o almacenar cualquier información confidencial o sensible sin la autorización correspondiente, tanto otorgada como parte de su trabajo, rol o por su gerente de línea.
- Acceder, almacenar, enviar, compartir o publicar:
- Imágenes o textos pornográficos, que contengan sexo explícito o sexo coactivo (incluyendo imágenes sexualmente abusivas de niños y niñas). Si los tipos de material accedido son considerados de naturaleza grave, SCI tiene la obligación de notificar a las agencias de seguridad.
- Materiales que promuevan la violencia, el odio, terrorismo o la intolerancia de otros
- Material que sea acosador, obsceno, abusivo o inconsistente con el Código de Conducta o cualquier normativa local.
- Instalar o usar software de aplicaciones no autorizados o prohibidos.
- Configurar su cuenta de correos de SCI para reenviar automáticamente contenidos de correo electrónico a cuentas de correos externas a SCI.

- Usar aplicaciones de la nube que no hayan sido aprobadas por el **Servicio de TI** para distribuir, almacenar o hacer copias de seguridad de información de SCI. Por favor, contactar con su soporte de TI o escribe a 'itsecurity@savethechildren.org' para mayores orientaciones sobre protección de la información de SCI mantenida en los Sistemas de TI.

Uso limitado, ocasional de los sistemas y servicios de TI de SCI para asuntos ajenos al trabajo es permitido; sin embargo, usted no debe:

- Usar una cantidad inaceptable de los recursos de los sistemas y redes de SCI para uso personal (p.e. uso excesivo de impresoras de SCI).
- Descargar o almacenar archivos grandes o transmitir audios o videos para uso personal (p.e. software o películas pirateadas).
- Permitir que el uso personal interfiera con su productividad o con la productividad de otros durante el trabajo.
- Usar indebidamente sistemas y servicios de tecnología de SCI para dirigir o apoyar un negocio privado.
- Usar indebidamente sistemas de SCI para participar en juegos o apuestas online.
- Distribuir spam o publicidades no deseadas usando el correo electrónico de SCI, p.e. enviar correo basura.
- Realizar cualquier actividad que pudiera dañar potencialmente la reputación de SCI.

Nota

La variabilidad y limitaciones del ancho de banda de red en diferentes sitios web podrían requerir mayores límites o restricciones en el permiso general del uso aceptable de activos de IT de SCI para propósitos personales.

El uso personal aceptable de TI de SCI en dichas circunstancias estará limitado a actividades online esenciales y/u ocasionales. Mayores restricciones específicas reflejarán las demandas sobre el ancho de banda disponible en cualquier circunstancia.

El uso personal aceptable de sistemas de TI de SCI incluye lo siguiente:

- Acceder a sitios web de noticias, clima, de planificación de vacaciones o información de viajes.
- Acceso ocasional a cuentas de correo personales en la web y sitios de redes sociales siempre que las instrucciones anteriores sean cumplidas.
- Uso ocasional de sistemas de TI para compras online.

4. Mantener seguros sus IDs de usuario y contraseñas

Las credenciales de acceso, tales como IDS de usuario, contraseñas, PINs o certificados digitales que utiliza para ingresar a los sistemas y servicios de TI de SCI no deben ser compartidos con ningún otro usuario/s. Consérvelos seguros y protegidos.

Usted:

- Nunca debe escribir contraseñas en notas autoadhesivas o papel y tenerlas en la laptop.
- Debe mantener en secreto las contraseñas y PINs y no debe compartirlos con nadie, incluyendo el servicio de TI y personas en su equipo.
- No debe permitir que nadie más use su cuenta de usuario sin su supervisión directa (p.e. si el servicio de TI arregla un problema en su sistema de TI).

Nota

- Siempre elija contraseñas fuertes que incluyan al menos ocho caracteres, con mayúsculas y minúsculas, cifras y caracteres especiales.
- Siga la política de cambio de contraseña: debe cambiar su contraseña cada 90 días.
- Revisar los Estándares Mínimos de Seguridad de TI para conocer la política de contraseñas y los requerimientos de cumplimiento.

5. Usar las redes sociales apropiadamente

Los contactos personales o anónimos en red pueden afectar la marca y reputación de SCI. No discuta ni comparta información de SCI que sea sensible, confidencial o de naturaleza interna en las redes sociales, por ejemplo, en blogs o sitios de microblogs, foros de debate, Facebook o Twitter.

Nota

- Nunca use su dirección de correo de SCI como identificador en páginas de redes sociales
- Nunca proporciones opinión/es de parte de SCI sin aprobación previa del personal autorizado. Si tiene dudas, contacte a su gerente de línea, comunicaciones internas globales o a un miembro del SLT.
- Si está autorizado, tome en cuenta del contenido de sus publicaciones en redes sociales con cuidado.
- Recuerde, cualquier publicación en redes sociales desde una computadora de SCI podría ser rastreada hasta su dirección IP original.
- Remitirse a la Política de Uso de Redes Sociales de SCI para mayor orientación

6. Gestionar cuidadosamente los riesgos a los sistemas de TI por el phishing, correos basura y virus

Los correos electrónicos no deseados (spam) y virus nocivos, troyanos, gusanos informáticos y programas espía pueden ocasionar una amenaza grave a nuestros sistemas de TI y a nuestra información.

Si usted no reconoce la fuente de un correo electrónico entrante:

- No abra ni guarde archivos adjuntos.

- No haga clic en los enlaces incrustados hacia otros sitios web.
- No responda correos electrónicos en busca de información personal o financiera.
- Desconfíe especialmente de enlaces que lo dirijan a un sitio web y que le pida ingresar si ID, contraseñas o información personal.

Nota

- Si usted recibe contenidos sospechosos incluyendo contenidos sobre el abuso de niños y niñas, repórtelo a 'itsecurity@savethechildren.org'.
- Elimine mensajes ofensivos o comerciales que promuevan o publiciten bienes, servicios u opiniones – el correo basura de Outlook puede ayudarlo a manejar esto. Si la frecuencia de dichos mensajes se convierte en un problema, contacte a Servicios de TI para asesoría.

7. Reportar incidentes de seguridad de TI inmediatamente

Es importante reportar cualquier infracción potencial o real de seguridad de TI para evaluar la solicitud de medidas adicionales a la vez que se protege nuestra información y sistemas de TI.

Reporte cualquier incidente de seguridad de TI y otros relacionados a 'itsecurity@savethechildren.org'.

Nota

Entre los ejemplos de incidentes de seguridad de TI denunciables se encuentran:

- Incumplimiento de esta política para el uso aceptable de TI o de los Estándares Mínimos de Seguridad TI.
- Cualquier robo o pérdida de computadora o dispositivo de almacenamiento que contenga cualquier tipo de información de SCI.
- Señales de accesos o acceso a archivos, por ejemplo, borrar/alterar archivos sin explicaciones.
- Iconos nuevos en máquinas de SCI o caídas del Sistema sin explicaciones.
- Ataques de malware/ransomware que afecten sistemas de TI de SCI.
- Pérdida o filtración de información sensible o confidencial a usuarios/sistemas ajenos a SCI sin autorización.
- Pérdida de documentos impresos que contengan información sensible o confidencial de SCI.

Reportar incidentes de Protección Infantil inmediatamente

Se le solicita que reporte cualquier infracción potencial o real a la Política de Protección Infantil y cualquier inquietud referida al abuso/daños posibles o reales contra niños y niñas para poder protegerlos a ellos, a nuestro personal y a la reputación de la organización como defensora de los derechos del niño.

Reporte cualquier incidente a childsafeguarding@savethechildren.org o a su punto focal o gerente de Protección Infantil.

Nota

Hay más información disponible en su Procedimiento de Protección Infantil local o del país para presentar una inquietud.

8. **Usar computadoras y teléfonos celulares provistos por SCI de manera segura y adecuada**

SCI provee sistemas de TI, incluyendo computadoras y teléfonos celulares (tales como laptops y teléfonos inteligentes) para uso de trabajo. Se ha dotado a estos sistemas de TI con los softwares necesarios para cumplir con el rol del puesto. Si usted requiere software adicional para desempeñar su rol, debe contactar a su **supervisor directo** o al **servicio de TI** y pedir asesoría.

Nota

Además de lo anterior, debe asegurarse de:

- El uso de sistemas de TI provistos por SCI cumple con los requerimientos en este documento.
- Usted no debe modificar ni retirar ninguna funcionalidad de seguridad preinstalada en los sistemas de cómputo, ni evitar que el aparato instale parches obligatorios y actualizaciones de seguridad.
- Su aparato se mantiene actualizado con las últimas actualizaciones de antivirus y de seguridad de malware.

Save the Children

DEFINICIONES

Palabra/Término	Definición
SCI	Save the Children Internacional
Sistemas de IT	Computadora, laptop, teléfono móvil, aplicación, software, servidor, aparatos de redes, servicios de Internet, impresoras, mensajería instantánea, lugar de trabajo (herramienta de colaboración), etc.
PII	Información Personalmente Identificable
SLT	Equipo de Liderazgo Senior
Dueño de la información	La persona(s) responsable de o conocedora de la forma en que la información es generada, creada, adquirida, transmitida, almacenada, eliminada o procesada
Usuario de la información	La persona(s), organización o entidad que interactúa con información con el propósito de realizar una tarea o procesamiento autorizado usando sistemas de TI
ISWG	Grupo de Trabajo de Seguridad de IT
HR	Recursos Humanos
RISC	Defensor Regional de Seguridad de la Información

Documentos de respaldo

1.	Política de TI – asegurar el abastecimiento, uso y protección de los Sistemas de TI y cualquier información procesada al usar estos sistemas.
2.	Política de Seguridad de TI – asegurar que los Sistemas de TI cumplen con los requerimientos de la Política de Información y Seguridad de TI, y con la gestión de cualquier excepción a esta política.
3.	Estándar Mínimo de Seguridad de TI – asegurar la concientización del usuario sobre seguridad de TI, controles y procesos de seguridad de TI son parte integral de nuestras responsabilidades operativas, de gestión y de gobernanza de TI.
4.	Política de Redes Sociales – asegurar el uso adecuado de redes sociales.