ALDEAS INFANTILES SOS INTERNACIONAL

REGLAMENTO DEL MANEJO Y SEGURIDAD DE LA INFORMACIÓN

Septiembre 2019- Versión 2.0

DOCUMENTO DE APOYO A LA POLÍTICA INTERNACIONAL

PUESTA EN PRÁCTICA LAS POLÍTICAS Y ESTÁNDARES DE CALIDAD

USUARIOS CLAVE

Obligatorio para:	*Colaboradores/as de la Secretaría General (colaboradores/as de Oficinas Regionales y de la Oficina Continental) y colaboradores/as de Asociaciones Nacionales en América Latina. Colaboradores/as contratados desde la oficina internacional se rigen sobre los reglamentos respectivos de esta unidad.*
Recomendado para:	

POLÍTICAS AFINES

Política fundamental:	*Information Security Global Policy* (https://intranet.sos-kd.org/areasofwork/ICT/Policies/Pages/IT-Security.aspx)
Política central:	
Estándares de calidad:	

DOCUMENTO HERRAMIENTAS, SISTEMAS AFINES

Estándar de clasificación de Información:	https://intranet.sos-kd.org/areasofwork/ICT/Policies/SOSDocuments/Information-Security-Classification-Standard-V1.pdf

RESPONSABLE DEL CONTENIDO

Área funcional:	Sergio Fernández
Departamento:	ICT

PROCESO DE DESARROLLO

Aprobado por:	CMT
Idioma original:	Español
Dirección de la intranet:	

HISTORIAL DEL CAMBIOS

Versión	Fecha	Cambios
1.0	Septiembre 2013	Primera versión del Documento
0.4	Agosto 2013	Correcciones solicitadas por CMT
0.3	Julio 2013	Correcciones solicitadas por las funciones
0.2	Marzo 2013	Edición de Borrador en base a primer control
0.1	Marzo 2013	Primer borrador de Documento creado

ÍNDICE

Resumen ejecutivo

¿Por qué la seguridad de información es importante?
Son varios los casos de situaciones que causaron daños e incluso impactaron económicamente a empresas/instituciones/organizaciones, resaltando la necesidad de tomar acciones que prevengan/minimicen dichos daños y riesgos.

Es imperioso el implementar mecanismos que protejan la información permitiendo garantizar la confidencialidad de los datos con los que trabajamos; de igual modo, resulta vital alinearnos al cumplimiento de regulaciones y leyes de gobiernos respecto a la seguridad de información y la protección de datos confidenciales ante pérdidas, robos, etc.

El buen resultado de dichos mecanismos y regulaciones puede alcanzarse mediante una activa gestión de seguridad de información en todas las funciones y gerencias de la Organización, no confundiendo este término con el de “seguridad informática” pues el control/protección va más allá de la información almacenada en medios informáticos.

Seguridad de IT no es solo un tema a abordarse en ICT, este es un tema relacionado a todas las áreas y gerencias de la organización. Todo el personal que gestiona, colecciona y administra información (información de participantes, donantes, etc.) debe cumplir con sus obligaciones acerca de la protección de datos según regulaciones locales, actualmente la mayoría de las leyes responsabiliza de manera personal a las gerencias sobre el manejo inadecuado de información, más allá de las leyes es un compromiso ético de la organización el uso adecuado de información. Es por esto que el contenido del presente documento debe ser tomado como normas mínimas a ser aplicadas, pudiendo las mismas ser ampliadas acorde a las normas de la AN/OR/OC e incluso las leyes del País.

Una brecha de seguridad puede ocurrir en cualquier momento. Pero cuando esta se da por negligencia puede traer un impacto catastrófico para Aldeas Infantiles SOS. Por ejemplo daño en la reputación de la organización ocasionando una devaluación de la marca, pérdida de confianza pública, reclamos de donantes y deserción, pérdida de ingresos, acciones legales por daños a terceros, etc. Interrupción de rutinas organizacionales serían las consecuencias menores

1 Acuerdo de Conformidad

Todos/as los/las colaboradores/as de Aldeas Infantiles SOS, consultores, contratistas y proveedores que tienen o intercambian información y realizan negocios con Aldeas Infantiles SOS deben cumplir con las regulaciones indicadas en este documento y ampliadas en https://intranet.sos-kd.org/ServiceTools/Helpdesk/ICT-Helpdesk/IT-Security/Pages/default.aspx

Daños causados por negligencia de los colaboradores los hacen propensos/sujetos a acciones legales y sus consecuencias según su cargo y responsabilidad. Consultores, contratistas y proveedores estarán sujetos a la terminación de sus contratos o el requerimiento de separar al agraviante individual que esté relacionado con Aldeas Infantiles SOS

2 Normas esenciales de seguridad de la información

2.1 Copias de Respaldo

Se refiere a la copia de seguridad de datos (documentos, bases de datos, correo electrónico, sistemas operativos, etc.) en un medio externo que posibilite su recuperación ante cualquier falla.

- Es necesario el contar con un sistema de archivos correctamente implementado
- Se debe procesar copias de respaldo de la información de cada usuario/a (documentos/correo electrónico), sistemas/bases de datos, etc.
- No se tomará en cuenta la elaboración de copias de respaldo de sistemas operativos (Windows XP/7, etc.).
- Dentro de la política de copias de respaldo se incluyen computadores de escritorio, equipos portátiles, dispositivos móviles y servidores.
- Los aspectos técnicos de las copias de respaldo (tipo de sistema, pasos a seguir, etc.) deben ser facilitados por el personal ICT de la ON/OR/OC.

2.1.1 Características que debe tener una copia de respaldo

Una copia de respaldo debe cumplir las siguientes características:

- Las copias de respaldo elaboradas deben ser almacenadas en un lugar seguro el cuál no debe encontrarse dentro del mismo ambiente del servidor o equipo del cual se respaldaron los datos.
- Debe contarse con una copia en un medio externo (Cintas, DVD, ZIP, CD, etc.).
- Las copias de respaldo deben ser realizadas por lo menos una vez por semana y es recomendable elaborarlas también antes de realizar un viaje.
- Solamente debe incluirse en las copias de respaldo información relacionada con la organización, por favor abstenerse de incluir información personal.
- En las copias de respaldo debe ser incluida solamente información que haya variado desde la copia anterior.
- De preferencia las copias de respaldo deben ser elaboradas fuera del horario de trabajo, esto para asegurarse que la información/sistemas no están siendo utilizados/as.

Los/las usuarios/as son responsables por:

- La información que se genera/administra en sus áreas de trabajo y el correcto manejo de la misma.
- El cumplimiento de las normas y procesos para la adecuada creación de las copias de respaldo.

El personal de ICT es responsable por:

- El correcto funcionamiento de los sistemas de copias de respaldo y servidores de archivos.
- La copia de datos en medios externos.
- Monitorear que los datos incluidos en las copias de respaldo solo incluyan información referente a la organización.
- La verificación de que las copias de respaldo han sido correctamente elaboradas.
- La capacitación a los/las usuarios/as, en el correcto manejo del sistema de copias de respaldo.
- Apoyar en la restauración de datos de los/las usuarios/as en caso de pérdida de información

2.2 Contraseñas seguras

Se denomina “contraseña segura” al conjunto de caracteres con los que usted puede autenticarse para ingresar a computadores, sistemas, bases de datos, su correo electrónico, etc. Este conjunto de caracteres es personal y no debe ser conocido por otras personas de otra manera deja de ser “seguro”. Cuan fácil es recordar una contraseña generalmente significa que es más sencilla su vulneración, por razones de seguridad es necesario reforzar las contraseñas cumpliendo con ciertos criterios de complejidad.

Algunos aspectos que debe recordar con respecto a las contraseñas en Aldeas Infantiles SOS:

- Cambiar las claves de acceso a computadores, sistemas, intranet, bases de datos, etc. Por lo menos cada tres meses, recuerde que no es posible utilizar las últimas dos contraseñas que ya haya sido utilizada.
- “Todos los computadores” de la organización deben contar con una contraseña de acceso y de descanso de pantalla (screensaver)
- Las contraseñas deberán ser cambiadas cada 3 meses

2.2.1 Características de una contraseña segura

Una contraseña segura debe cumplir las siguientes características:

- Debe tener como mínimo 10 caracteres de longitud.
- No se deben utilizar nombres o palabras fáciles de recordar (Ej. SOS, KDI, LASO, LACE, etc.).
- No se deberá reutilizar una contraseña.
- Las contraseñas no deberán ser escritas en papel ni guardadas cerca del computador (no pegarlas en el monitor).
- La contraseña debe contener por lo menos 4 de las siguientes 5 categorías
    - Caracteres en mayúsculas (A-Z)
    - Caracteres en minúsculas (a-z)
    - Dígitos de base 10 (0-9)
    - Caracteres no alfanuméricos (ejemplo: !, $, #, %, etc.)

- Caracteres Unicode
- La contraseña no debe contener tres o más caracteres provenientes del ID del usuario

Los/las usuarios/as son responsables de:

- El manejo y creación de las contraseñas.
- Notificar al personal ICT ante la pérdida o uso no autorizado de su ID de usuario o contraseña, si hubiera sido necesario facilitar la contraseña a un tercero o alguna otra brecha de seguridad.
- No proporcionar su ID de usuario o contraseña a ninguna persona, compañías u organizaciones dentro o fueras de Aldeas Infantiles SOS
- No almacenar su ID de usuario o contraseña en su computador o en sistemas externos, no envíe sus contraseñas mediante servicios sin encriptación como E-mail, FTP, HTTP no seguro, etc.
- No escribir en ningún lado su ID de usuario o contraseña, especialmente en lugares visibles como cuadernos, post-its, block de notas en el computador, etc.
- manténgalos en su mente

El personal ICT es responsable de:

- Aplicar las políticas de seguridad respecto al uso adecuado de contraseñas
- El control del tiempo de validez de las contraseñas.
- La capacitación a los/las usuarios/as, en el correcto manejo/administración de las contraseñas.
- Apoyar a los/las usuarios/as en el cambio de su contraseña. en caso de pérdida de la misma

2.2.2 Recomendaciones

Para mayor información al respecto le recomendamos consultar las siguientes direcciones
http://hotfixed.net/2010/10/20/como-crear-y-recordar-passwords-seguros/

2.3 Uso de Internet y Correo Electrónico

2.3.1 Uso de Internet

- Cualquier actividad en Internet o uso de correo electrónico de parte de colaboradores de Aldeas Infantiles SOS que pudiera tener un efecto negativo en Aldeas Infantiles SOS es, sin ninguna excepción, prohibida

  Lugares con un impacto negativo a Aldeas Infantiles SOS incluyen entre otras:
  - Páginas de contenido pornográfico, especialmente de niños/as.
  - Páginas ligadas a grupos terroristas.
  - Páginas que presenten, promuevan o anuncien juegos, libros, películas, etc. Enalteciendo la violencia.
  - Sitios de partidos políticos o grupos que han sido prohibidos en el mundo o vulneren el reconocimiento de los derechos humanos (ejemplo NSDAP).
  - Sitios de sectas religiosas/religiones no oficiales que vulneren el reconocimiento de los derechos humanos o que promuevan actividades prohibidas por legislaciones locales.
  - Páginas que atenten la dignidad de personas o animales.
  - Sitios de piratería informática (con la excepción de personal ICT que lo requiera por motivos de trabajo).
- Los/las colaboradores/as dentro del horario de trabajo no deben hacer uso del Internet para asuntos personales.
- Es prohibido el uso de Internet para sintonizar radio/televisión, escuchar música, visualización de videos que no sean referentes a su trabajo.
- No está autorizado el descargar películas, música, imágenes, programas que no sean referentes a su trabajo.

2.3.2 Correo electrónico

- El envío o reenvío de correo basura (SPAM) o correo con publicidad masiva no solicitada (Junk Mail) está prohibido, especialmente correos no deseados, comerciales, cadenas, etc.
- No se deberá utilizar la cuenta corporativa para publicar mensajes en foros de discusión que no tienen relevancia con su trabajo, publicar información en foros acerca de política, deportes, pasatiempos, etc.
- Está prohibido el uso de servidores de correo externos como estaciones de distribución (relay) para el envío de correo electrónico sin el permiso expreso del dueño/a de la cuenta
- Salvo autorización, se solicita a los/las colaboradores/as no enviar correos electrónicos en nombre de otras personas.
- Los archivos adjuntos no deben ser mayores a 3 MB, si necesita enviar correos de mayor tamaño utilice enlaces (links) generados por Onedrive, contacte a su personal ICT para mayores detalles o apoyo.
- Regularmente elimine correos no deseados, esto le permitirá contar con mayores recursos en el computador.

2.4 Redes sociales Facebook, Twitter, etc.

(En esta sección no se contempla lo referente al manejo de recaudación de fondos digital)

Las redes sociales como Facebook, Twitter, LinkedIn, Yammer, etc. pueden proveernos muchos beneficios. Pero junto a estos beneficios hay aspectos de seguridad que deben ser tomados en cuenta antes de adoptarlas.

A tomarse en cuenta cuando “hablamos” de Aldeas Infantiles SOS en las redes sociales:

- Aclare que las opiniones son personales y no son en nombre de la organización.
- Asegúrese de proveer información valiosa y contenido alineado con su trabajo en Aldeas Infantiles SOS y la marca de Aldeas Infantiles SOS. Tenga presente que usted es parte de la marca y por consiguiente responsable de los NNAJs en riesgo, las 24 horas del día.
- Hable acerca de:
    - El core (núcleo) de nuestro trabajo y nuestra identidad única
    - Los valores de Aldeas Infantiles SOS
    - Los NNAJs en riesgo y su desarrollo individual
    - Los significados que queremos compartir
    - Nuestra experticia y el enfoque centrado en las aldeas y los NNAJs

En general no está permitido el uso de términos y actividades que pudieran tener un efecto negativo en Aldeas Infantiles SOS, otros aspectos que deben ser considerados son:

- No utilice redes sociales personales para actividades de marketing o relaciones públicas
- Tenga cuidado pues las ideas personales de líderes de la organización pueden ser considerados posiciones de Aldeas Infantiles SOS
- No provea información que ha sido clasificada para Uso Interno, Confidencial o Estrictamente Confidencial, mayor referencia https://intranet.sos-kd.org/areasofwork/ICT/Policies/SOSDocuments/Information-Security-Classification-Standard-V1.pdf
- No difunda rumores y evite hacer comentarios acerca de estos
- Evite la publicación de comentarios sobre temas delicados como ser religiosos o políticos
- Si encuentra en alguna red social información o aseveraciones que considere directamente negativas para Aldeas Infantiles SOS, notifíquelo a una autoridad superior tan pronto le sea posible.

2.5 Uso de computadores

Los equipos de computación provistos por la organización son para uso exclusivo de trabajo

No está permitida la instalación de programas que no son aprobados por ICT de Aldeas Infantiles SOS y no está permitida la modificación de las configuraciones o políticas aplicadas por Aldeas Infantiles SOS

Por razones de seguridad todos los computadores deben contar con seguridad ante ausencia del responsable, favor verifique la parte referente a contraseñas en equipos y protectores de pantalla

Fuera de horas de trabajo los computadores de escritorio deben permanecer apagados, esto permite que al iniciarse se asegure las actualizaciones de parches de seguridad y por otro lado extiende el tiempo de vida útil de un equipo y genera ahorro en energía.

2.6 Protección contra virus

Incluso si un programa antivirus es constantemente actualizado, no ofrece absoluta protección contra virus de computadores, gusanos y software malicioso. Un sistema está expuesto a nuevos virus hasta que los fabricantes de software antivirus hayan desarrollado y provisto las firmas antivirus apropiados

Un virus de computador puede, dependiendo de su propósito, causar diferentes tipos de daño, algunos solo se replican y en algunos casos generan carga de trabajo en el computador deteriorando las rutinas diarias de trabajo, algunos al activarse destruyen información o despliegan mensajes o imágenes en la pantalla, etc.

2.6.1 Prevención contra virus

- Bajo ninguna circunstancia debe deshabilitarse el programa antivirus
- No cambiar ninguna de las configuraciones del programa antivirus
- No instalar ninguna aplicación, sistema o programa no autorizado y relevante a su trabajo en el computador
- No abrir archivos adjuntos en correos electrónicos que tienen un origen desconocido, sospechoso o de un origen poco formal/confiable
- No abrir archivos de correos electrónicos a menos que usted conozca su referencia, incuso si vienen correos electrónicos desde amigos o conocidos. Algunos virus pueden auto replicarse y distribuirse por correo electrónico
- No abrir ningún correo electrónico si la línea de asunto es cuestionable o no confiable
- Elimine correos electrónicos que son cadenas y correos electrónicos de publicidad. No reenvíe o responda a ninguno. Estos tipos de correos son considerados correo basura (SPAM)
- Sea cuidadoso con los correos “engaño” (HOAXES), ellos contienen información falsa que solo pretende atemorizar o confundir a los usuarios, simplemente elimínelos

2.7 Encriptación de datos confidenciales

Información que es clasificada como confidencial por Aldeas Infantiles SOS debe ser encriptada antes de su transmisión por canales no seguros como internet o antes de su transporte por medios que pueden perderse fácilmente como ser memorias USB o discos duros externos

Aldeas Infantiles SOS ha clasificado en cuatro los niveles de información, estos son: Público, De Uso Interno, Confidencial y Estrictamente Confidencial, en la siguiente dirección usted puede encontrar el detalle y el significado de cada uno de los niveles https://intranet.sos-kd.org/areasofwork/ICT/Policies/SOSDocuments/Information-Security-Classification-Standard-V1.pdf , solamente información que es clasificada como Confidencial o Estrictamente confidencial debe ser encriptada antes de su transmisión mediante un canal no seguro.

2.7.1 Canales no seguros

En general todos los canales de información fuera de las redes IT de Aldeas Infantiles SOS son considerados no seguros. Por ejemplo estos canales pueden ser móviles como memorias USB, discos duros externos o canales electrónicos como e-mail, FTP, HTTP no seguro, o plataformas externas como Skydrive, Dropbox o Apple iCloud

2.7.2 Como encriptar información

Aldeas Infantiles SOS confía en la herramienta Axcrypt, fácil de utilizar y software de encriptación que no requiere de licencia de uso para Windows XP/7. Además de su integración directa en Windows Explorer, posibilitando la encriptación, des encriptación, vista preliminar y edición de cualquier archivo, más información e instrucciones pueden encontrarse en: https://intranet.sos-kd.org/ServiceTools/Helpdesk/ICT-Helpdesk/IT-Security/Pages/ITSEC-enrypt-decrypt.aspx

2.8 Ingeniería social

Son actos que tratan de obtener información confidencial mediante engaños. La ingeniería social es exitosa porque las víctimas de manera innata confían en otras personas, ingeniería social es el acto de intrusión a personas en lugar de computadores

2.8.1 Como evitar la ingeniería social

- Sospeche de llamadas telefónicas o visitas no solicitadas/coordinadas, ejemplo una persona visita las oficinas solicitando información referente a colaboradores/as
- No provea información personal o de la organización a menos que esté completamente seguro de que se trata de alguien con los roles y permisos para tenerla
- No revele información sensible personal o financiera vía correo electrónico
- Preste atención a las direcciones de internet de páginas web externas
- Nunca provea fuera de la organización información como nombres de usuario, números ID, números de PIN, nombres de servidores, sistemas de información, números de tarjetas de crédito, etc.
- Si le solicitan información confidencial por teléfono, esté seguro de que quien la pide es de una unidad/oficina/equipo confiable. Ejemplo si es información solicitada por auditores externos o personal técnico de ICT
- Tenga cuidado con los archivos adjuntos que quieran ejecutar procesos no autorizados en su computador, no acepte requerimientos de información de cuentas como contraseñas
- Tenga cuidado de lo que se le pide en persona, nunca se sienta presionado si la persona le dice “sabe quién soy yo?”, solicite por un contacto para verificar

2.9 Información no electrónica

Documentación física, como documentos impresos, contienen también información crítica de la organización y deben ser protegidos de manera adecuada de accesos no autorizados

Documentación no electrónica como contratos, formularios, certificados, balances financieros, etc. Contienen información sensible como números de cuentas bancarias, tarjetas de crédito, información de donantes, políticas, estrategias, manuales, etc. Que debe ser salvaguardada por el responsable definido en cada función siguiendo los métodos indicados por la misma (ej.: archivos físicos bajo llave, eliminación adecuada de impresiones no válidas con información sensible, etc.)

Se considera información crítica no electrónica según la clasificación de los cuatro niveles de información, mayor información en: https://intranet.sos-kd.org/areasofwork/ICT/Policies/SOSDocuments/Information-Security-Classification-Standard-V1.pdf , adicionalmente se incluye otro tipo de documentación que no esté en esta clasificación pero que este protegida por leyes locales

2.10 Dispositivos móviles

Dispositivos móviles como ser computadores portátiles, teléfonos móviles, tabletas, memorias USB, discos duros externos, etc. son blanco de muchos tipos de ataques e intrusiones

Esto hace de ellos una brecha importante en aspectos de seguridad, es más fácil el acceso a ellos que a dispositivos dentro de nuestra red corporativa.

Todos los colaboradores/as que tienen a su cargo dispositivos móviles deben ser conscientes que estos son dispositivos que atraen a ladrones por su fácil manejo y posibilidades de venta, aparte de los costos más elevados. La pérdida de información confidencial en estos equipos puede causar grandes daños a la organización, por consiguiente se sugiere inicialmente, por parte del colaborador/ra a cargo, la asignación de una contraseña al dispositivo móvil tomando en cuenta las características de contraseñas seguras explicadas en el presente documento y, por parte de la Organización, el asegurar el traslado de estos equipos para eventos de orden laboral, manteniéndose los mismos bajo cuidado de su responsable no debiendo dejarse sin atención o desprotegidos por largos periodos de tiempo

2.10.1 Asegurar información sensible

Con el fin de prevenir el acceso a información sensible de personal o terceras partes no autorizado/as en dispositivos móviles, todos los colaboradores de Aldeas Infantiles SOS, consultores, proveedores de servicios y contratistas que manejan e intercambian información con Aldeas Infantiles SOS son responsables por la asignación de una contraseña segura al dispositivo móvil y una adecuada encriptación de información, la cual responde a nuestros estándares de clasificación de información confidencial, mayores detalles en: https://intranet.sos-kd.org/areasofwork/ICT/Policies/SOSDocuments/Information-Security-Classification-Standard-V1.pdf

Computadores portátiles implementadas por nuestro personal de ICT y que gestionan datos sensibles vienen usualmente con software de encriptación. Por favor refiérase a su equipo de ICT local.

Adicionalmente tome en cuenta que es su responsabilidad asegurar datos confidenciales que le hayan sido transferidos por medios no seguros, como ser e-mail. FTP, etc. O almacenados en plataformas externas como Microsoft SkyDrive, Dropbox o Apple iCloud

Información clasificada como Confidencial o Estrictamente Confidencial debe ser sacada de nuestra red corporativa solo en casos en los que son “absolutamente necesarios” y siguiendo todas las regulaciones mencionadas en este documento

2.11 Gestión de Usuarios

El número de aplicaciones, sistemas y BDs es cada vez mayor y los accesos de los colaboradores/as a estas herramientas requieren de una adecuada gestión tanto en la creación y mucho más en la eliminación de accesos no autorizados.

Al ingresar un/a colaborador/a a la Organización, le es creado un usuario con permisos básicos a intranet y una cuenta de correo electrónico. Los procesos de creación, administración y eliminación de usuarios de Aldeas Infantiles SOS, son gestionados por el área de RR.HH./D.O. en la AN/OR/OC.

En caso de que el/la colaborador/a requiera acceso a otros sistemas (Lucy, Teamsites, etc.), deberá solicitar al área que corresponda los respectivos permisos contando con el aval de su supervisor/a directo. En caso de darse la salida/el egreso del/de la colaborador/a, el supervisor/a directo deberá definir el plazo por el cual se redirigirá el correo electrónico en caso de ser necesario (llegado el momento, se procederá con la eliminación del mismo) y luego de realizada la solicitud correspondiente, RR.HH./D.O. dará de baja el acceso a Intranet como medio preventivo por el buen resguardo de la información de la Organización.

2.12 Responsabilidades

Es responsabilidad de los directores (de programas/nacionales/regionales/continental) y los Asesores/Directores de funciones/áreas de trabajo y equipo de ICT el cumplimiento de las normas indicadas en el presente documento.

2.13 Siglas utilizadas en el documento

HTTP	Hipertext Transfer Protocol
FTP	File Transfer Protocol
BD	Base de Datos