



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 1 de 8

16 .SEGURIDAD INFORMÁTICA

16.1 POLITICA DE SEGURIDAD INFORMATICA

En el Hospital Infantil Los Ángeles todos los usuarios somos responsables de la información automatizada que manejamos y debemos dar estricto cumplimiento a los lineamientos generales y especiales dados por la organización, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Toda persona que utilice los servicios informáticos del Hospital, deberá conocer y aceptar la política sobre su uso, el desconocimiento de la misma, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

16.2 ALCANCE

Este documento proporciona instrucciones definitivas de las políticas de seguridad informática que aplica a todos los trabajadores que estén involucrados con el manejo de información.

16.3 OBJETIVOS

- Conocer la importancia de la información y los mecanismos para propiciar su manejo seguro.
- Familiarizar a los trabajadores con los riesgos en seguridad informática y las maneras que se espera sean atendidos dichos riesgos.
- Clarificar las responsabilidades y deberes del trabajador con respecto a la protección de los recursos informáticos.
- Sustentar el apoyo constante del direccionamiento estratégico a esta política de seguridad de información.
- Facilitar la toma de decisiones por parte de la gerencia y otros trabajadores en materia de seguridad informática.
- Sensibilizarse en que la seguridad de la información se consigue entre todos los usuarios y no es solo una labor del personal de gestión de información.
- Coordinar los esfuerzos de las distintas áreas del Hospital Infantil Los Ángeles de manera de proteger de forma consistente los recursos informáticos, sin importar su ubicación, forma o plataforma tecnológica.

16.4 USO DE EQUIPOS DE CÓMPUTO

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------



HOSPITAL INFANTIL LOS ANGELES

Código: OD08_GI V5

Fecha: 15 Enero de 2019

PLAN DE GERENCIA DE LA INFORMACION

Responsable: Subgerente de información y sistemas

Página: 2 de 8

El propósito de esta política es establecer las directrices y los requisitos para asegurar la protección apropiada de la información del Hospital al trabajar con equipos de cómputo.

- Los computadores, periféricos y software son de uso exclusivo del personal del Hospital para el desarrollo de sus funciones y responsabilidades establecidas por y para la Institución.
- Los usuarios no pueden modificar la configuración de hardware y software establecida por el área de sistema de información.
- Los usuarios deben cumplir a cabalidad con las normas básicas de cuidado de los equipos entregados, como son:
 - a) No ingerir, ni dejar alimentos y/o bebidas cerca y/o encima de los equipos
 - b) No fumar ni ubicar ceniceros cerca y/o encima de los equipos.
 - c) Facilitar la ventilación del equipo, no colocar papeles u otros objetos cerca a las ranuras de ventilación del equipo.
 - d) No colocar objetos pesados, encima de la unidad central de proceso (CPU), a fin de evitar su deterioro o maltrato
 - e) Mantener alejados de la CPU, monitor y pantalla todo elemento electromagnético como imanes, teléfonos, radios, entre otros.
 - f) No colocar la Unidad Central de Proceso (CPU), en el piso o lugares inestables y/o expuestos a ser golpeados involuntariamente
 - g) No trasladar ni mover los equipos y/o periféricos de un lugar a otro. En caso de ser necesario el traslado, se debe informar al área de sistemas para que se revisen las condiciones técnicas necesarias del nuevo lugar.
 - h) No abrir los equipos de cómputo. En caso de ser necesario, se debe comunicar al área de sistemas.
 - i) Conservar limpio el teclado, monitor y mouse mediante limpieza externa.
 - j) Conservar los cables en buen estado, ordenados y correctamente conectados; no debe de existir ningún tipo de tensión, evitando el doblado de los mismos.
 - k) No colocar la punta de los dedos, lapiceros u objetos metálicos en el vidrio del monitor para señalar la pantalla
 - l) Ubicar y mantener el equipo alejado del polvo y la luz solar directa.
 - m) No conectar ventiladores u otros aparatos con motor eléctrico en los mismos enchufes o líneas de los equipos de cómputo.
- Deben usarse protectores contra transitorios de energía eléctrica (reguladores) en los puntos donde no se cuente con corriente regulada y en los servidores deben usarse fuentes de poder interrumpibles (UPS).
- Toda falla de los equipos o de la red debe ser reportada al área de sistemas de información ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Los equipos serán marcados para su identificación y control de inventarios.
- Los equipos no podrán salir del Hospital sin previa autorización escrita del Jefe inmediato y visto bueno del subgerente de gestión de información.

Elaboró: ALEXANDER ACOSTA
Actualizó: ALEXANDER ACOSTA

Revisó :CARLINA DOMINGUEZ T.

Aprobó: DORIS SARASTY R.



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 3 de 8

- Para la adjudicación de equipos nuevos se debe hacer la solicitud por escrito a el área de sistemas con el visto bueno del Jefe inmediato, se procede a entregar el computador mediante acta, con el respectivo visto bueno de suministros para el plaqueteo del activo e ingreso al inventario de sistemas; previa entrega del equipo a reemplazar por parte del solicitante, en caso de reemplazo.
- La información confidencial que aparezca en pantalla debe protegerse de ser vista por otras personas mediante la disposición apropiada del mobiliario de la oficina y protector de pantalla.
- La información obtenida y desarrollada en el cumplimiento de las funciones es propiedad intelectual de la institución, la cual no deberá ser distribuida, comercializada ni divulgada
- El software del Hospital está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- Los usuarios solo podrán tener instalados en sus computadores: software, aplicativo y/o sistemas autorizados por la subgerencia de gestión de información en concordancia con las disposiciones de la gerencia del Hospital.
- No se permite el ingreso de copias piratas o ilegales.
- Todos los usuarios antes de ingresar cualquier medio extraíble de almacenamiento (Disquete, CD, DVD, memoria USB) deben hacer la revisión de los mismos con el software antivirus del que disponga el Hospital. En caso de detectarse la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de sistemas de información.
- Está prohibido instalar: Software no licenciado incluido el que haya sido adquirido por el propio usuario, Chat (MSN Messenger, ICQ, Yahoo Messenger, etc, protectores de pantalla (sólo los autorizados por la subgerencia de gestión de información), Juegos, software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la subgerencia de gestión de Información; en caso de encontrar software no autorizado será desinstalado y el responsable del equipo será informado a la subgerencia de gestión humana.
- La subgerencia de gestión de información es la única autorizada para instalar cualquier tipo de software, para lo cual el usuario debe hacer la solicitud a dicha UBG por escrito.
- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilancia privada, cerradura con llave y cámaras de video con grabación continua.

16.5 USO Y ADMINISTRACION DE REDES

El propósito de esta política es establecer las directrices y los requisitos para asegurar la protección apropiada del Hospital al estar conectado a redes de computadores.

Modificaciones: Todos los cambios en los servidores y equipos de red del Hospital, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Lo anterior con el fin de evitar problemas por cambios apresurados

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 4 de 8

que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios:

- La solicitud de una nueva cuenta o usuario, el cambio de privilegios o perfiles debe hacerse por escrito y estar debidamente aprobada por el jefe inmediato.
- No se concederán cuentas a personas que no sean empleados del Hospital a menos que estén debidamente autorizados, en cuyo caso la cuenta expirara automáticamente al cabo de 30 días.
- No se otorgaran cuentas a técnicos de mantenimiento, ni se permitirá su acceso remoto a menos que el subgerente de gestión de información determine que es necesario. En caso de presentarse la necesidad debe habilitarse una cuenta para el periodo de tiempo requerido para efectuar el trabajo (mantenimiento remoto).
- Está prohibido el uso de cuentas anónimas o de invitados y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto implica que los administradores de servidores de sistemas Linux deben entrar empleando su propio ID, luego obtener acceso como "root".
- Cuando un empleado se desvincule del Hospital Infantil Los Ángeles, su cuenta debe desactivarse antes de que deje el cargo, previo informe de la subgerencia de gestión humana a la subgerencia de gestión de información.

Contraseñas y el control de acceso

- La contraseña entregada a los usuarios es de carácter confidencial, por lo tanto, no debe ser guardada en medios físicos o magnéticos de fácil acceso, compartirse o revelarse a otros. El usuario que dé a conocer su contraseña se hace responsable por las consecuencias de las acciones que los demás hagan con esa contraseña.
- La contraseña entregada inicialmente es válida para la primera sesión, dentro de la cual debe ser cambiada.
- Si hay razón para creer que una contraseña ha sido conocida por otros usuarios, el usuario debe cambiarla inmediatamente y se recomienda no utilizar contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe evitarse usar contraseñas anteriores.
- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switches, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- El sistema de información Hosvital informa faltando siete días la expiración de la contraseña de usuario, de acuerdo al tiempo establecido por el área de sistemas, por lo tanto antes de que se cumplan los siete días los usuarios deben cambiar su contraseña, de lo contrario el usuario se inactiva.
- Los servidores de red y los equipos de comunicación serán ubicados en centros de cómputo apropiados, protegidos contra daños y robo.
- Está restringido el acceso a personal no autorizado a los centros de cómputo y a los cuartos de cableado.

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 5 de 8

16.6. MANEJO DE COPIAS DE SEGURIDAD

El propósito de esta política es establecer las directrices y los requisitos para asegurar la protección apropiada de la información almacenada en los computadores del hospital.

- Para la aplicación de esta política se debe remitir al procedimiento PR05_GI de copias de seguridad.

16.7 USO DE INTERNET

El propósito de esta política es establecer las directrices y los requisitos para orientar el uso de internet únicamente con fines institucionales.

- El servicio de internet no debe ser usado para fines personales, y queda estrictamente prohibido utilizar descargadores de música, videos, software, escuchar música o ver videos en línea, visitar páginas para adultos y/o sexo explícito.
- La asignación de acceso a Internet, debe ser solicitada a la subgerencia de gestión de información. Esta solicitud se debe realizar a través del formato de mantenimiento correctivo.
- La subgerencia de gestión de información se encargara de administrar el servicio de internet, por lo cual deberá monitorear, controlar o bloquear páginas de ser necesario, con el fin de disminuir riesgos para la seguridad de la información del Hospital.
- En caso de violación a las políticas de internet, se suspenderá el servicio durante una semana y en caso de repetirse, se suspenderá el servicio de forma permanente.

16.8 USO DEL CORREO INSTITUCIONAL

Establecimiento de la Propiedad de los mensajes institucionales: Como herramienta para aumentar la productividad, disminuir los costos de uso de papelería e impresión y aportar a la conservación del medio ambiente, el Hospital Infantil Los Ángeles estimula el uso institucional de los sistemas de comunicación electrónica, especialmente la Internet, intranet y el correo electrónico. Salvo en el caso de que terceros hayan hecho valer sus derechos reservados, o algún otro derecho, en los mensajes manejados por estos sistemas, todos los mensajes generados o manejados por la Fundación Hospital Infantil Los Ángeles, se consideran propiedad de ésta.

Uso Autorizado: En términos generales, los sistemas de comunicación electrónica de la Fundación Hospital Infantil Los Ángeles deben usarse únicamente para actividades institucionales. El uso personal adicional no es permitido. Los sistemas de comunicación electrónica no deben usarse para la organización de campañas de recaudación de fondos para obras benéficas, actividades para la defensa de intereses políticos o religiosos, actividades privadas de negocios o entretenimiento personal. Las fuentes de noticias, listas de direcciones

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 6 de 8

de correo electrónico, actualizaciones automáticas de datos y otros mecanismos para la recepción de información a través de la Internet deben restringirse a materiales que estén relacionados directamente con la misión del Hospital Infantil los Ángeles y las tareas y funciones de los destinatarios. Se recuerda a los trabajadores que el uso de los recursos corporativos del sistema de información nunca debe crear la impresión o la realidad de que se están empleando indebidamente.

Privilegios Predeterminados: Los sistemas de comunicación electrónica deben establecerse y mantenerse de tal forma que solamente se otorguen al trabajador los privilegios necesarios para llevar a cabo su trabajo. Por ejemplo, al momento de terminar la relación entre el trabajador y la Fundación Hospital Infantil Los Ángeles también deben cesar todos los privilegios del trabajador en los sistemas de comunicación electrónica de la Fundación Hospital Infantil Los Ángeles.

Identificación de Usuarios: Para ingresar a los sistemas de correo electrónico deben utilizar los identificadores de usuario y las contraseñas correspondientes, asignadas por la subgerencia de gestión de información; los trabajadores no deben emplear el identificador de ningún otro usuario.

Responsabilidad del Usuario: Independientemente de las circunstancias, las contraseñas individuales nunca deben compartirse o revelarse a ninguna persona, excepto al usuario autorizado. Para impedir que partes no autorizadas obtengan acceso a las comunicaciones electrónicas, las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. Por ejemplo, los usuarios no deben incluir palabras que se encuentran en diccionarios, datos personales, nombres o algún otro término relacionado con las actividades del trabajo.

Identidad del Usuario: Queda prohibido falsear, confundir, ocultar o sustituir la identidad de otro usuario en un sistema de comunicaciones electrónicas. El nombre del usuario, la dirección de correo electrónico, la afiliación a una organización y otros datos relacionados incluidos en los mensajes o anuncios electrónicos deben señalar el verdadero origen de los mismos; los trabajadores no deben enviar comunicaciones electrónicas anónimas. Todos los mensajes deben incluir la plantilla configurada por la subgerencia de gestión de información que incluye como mínimo nombres, apellidos, cargo, dirección de la organización y número de teléfono.

Horarios de uso de los Sistemas de Correo Electrónico de la Fundación Hospital Infantil Los Ángeles:

Los trabajadores deben consultar sus cuentas de correo electrónico interno y externo según aplique, por lo menos dos veces diarias, una vez en la mañana y otra en la tarde con el fin de asegurar un canal de comunicación efectivo y oportuno.

Respeto a los Derechos de Propiedad Intelectual: Aun cuando la Internet es un ambiente informal de comunicaciones, también hay que cumplir las leyes de derechos reservados, patentes y marcas registradas. Los trabajadores que usen los sistemas de correo electrónico de la Fundación Hospital Infantil Los Ángeles solamente deben reenviar o reproducir material después de obtener el permiso de la fuente, citar material de otras fuentes sólo si éstas se

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------



HOSPITAL INFANTIL LOS ANGELES

Código: OD08_GI | V5

Fecha: 15 Enero de 2019

PLAN DE GERENCIA DE LA INFORMACION

Responsable: Subgerente de información y sistemas

Página: 7 de 8

logran identificar adecuadamente o revelar la información interna de la Fundación Hospital Infantil Los Ángeles en la Internet únicamente cuando haya sido autorizada oficialmente su divulgación pública. Toda información adquirida de Internet se debe considerar no confiable hasta que haya sido confirmada por otra fuente.

Respeto del Derecho a la Privacidad: Salvo que el gerente general lo autorice específicamente de otra manera, los trabajadores no deben interceptar, revelar, ni contribuir en la interceptación o revelación de las comunicaciones electrónicas. La Fundación Hospital Infantil Los Ángeles se compromete a respetar los derechos de sus trabajadores incluyendo el respeto a su privacidad e igualmente se responsabiliza de la operación, el mantenimiento y la protección de sus redes de comunicaciones electrónicas. Para alcanzar estos objetivos, en ocasiones será necesario interceptar o revelar o contribuir en la interceptación o revelación de las comunicaciones electrónicas, para lo cual la Fundación Hospital Infantil Los Ángeles puede emplear sistemas de evaluación de contenido, sistemas de registro de mensajes y otras herramientas de gestión de sistemas electrónicos. Al hacer uso de los sistemas de la Fundación Hospital Infantil Los Ángeles, los usuarios dan su consentimiento para que toda la información que ellos almacenen en los sistemas se divulgue a las autoridades pertinentes, a discreción de la gerencia de la Fundación Hospital Infantil Los Ángeles.

Contenido de los Mensajes: Los trabajadores no deben usar frases irreverentes, palabras obscenas o comentarios peyorativos en los mensajes de correo electrónico en referencia a los empleados, los clientes, los competidores u otras personas, ya que esos comentarios pueden crear problemas legales tales como la difamación y la calumnia en contra de empresas y personas. En las comunicaciones electrónicas de la Fundación Hospital Infantil Los Ángeles, los trabajadores deben ocuparse de los asuntos relacionados con la misión del Hospital. Todas las comunicaciones deben adherirse a las normas convencionales de conducta, de ética y de cortesía.

Divulgación Incidental: El personal de soporte técnico no debe revisar el contenido de las comunicaciones de un trabajador en particular, bien por simple curiosidad o a solicitud de individuos que no hayan utilizado los canales adecuados. Para realizar esta evaluación, se requiere una autorización previa del gerente general.

Respaldo del Usuario: Si un mensaje de correo electrónico contiene información esencial para completar una transacción de negocios, información de referencia de importancia potencial o que sea valiosa como prueba para sustentar decisiones tomadas por la gerencia de la Fundación Hospital Infantil Los Ángeles, se debe guardar para referencias futuras. Los usuarios deben trasladar con regularidad la información de los archivos de mensajes de correo electrónico a documentos procesados en texto, bases de datos y otros archivos. Las bandejas de entrada del correo electrónico no deben usarse para el almacenamiento de información importante, ya que no es un medio de almacenamiento sino un medio de comunicación.

Eliminación de Mensajes Electrónicos: Los usuarios deben eliminar periódicamente de sus espacios de almacenamiento los mensajes que ya no se necesiten para efectos institucionales, debido a que el espacio asignado en disco para cada cuenta de correo es limitado (200 megabytes).

Elaboró: ALEXANDER ACOSTA
Actualizó: ALEXANDER ACOSTA

Revisó :CARLINA DOMINGUEZ T.

Aprobó: DORIS SARASTY R.



HOSPITAL INFANTIL LOS ANGELES	Código: OD08_GI V5
	Fecha: 15 Enero de 2019
PLAN DE GERENCIA DE LA INFORMACION	Responsable: Subgerente de información y sistemas
	Página: 8 de 8

Materiales Ofensivos: Los sistemas de comunicaciones y de computación de la Fundación Hospital Infantil Los Ángeles no están destinados ni deben usarse para el ejercicio del derecho a la libre expresión del trabajador. Estos sistemas no deben usarse como un foro abierto para discutir cambios organizacionales de la Fundación Hospital Infantil Los Ángeles o asuntos de política de los negocios. Queda estrictamente prohibido el acoso sexual, étnico y racial a través del correo electrónico interno o externo. Los trabajadores que reciban material ofensivo no solicitado proveniente de fuentes externas no deben reenviarlo o redistribuirlo, bien sea a personas dentro de la empresa o a terceros, a menos que este reenvío o redistribución se haga a la subgerencia de Gestión Humana con el objeto de colaborar en la investigación de quejas.

Uso por Cuenta y Riesgo: Los trabajadores acceden a la Internet con las facilidades de la Fundación Hospital Infantil Los Ángeles bajo su propia responsabilidad. La Fundación Hospital Infantil Los Ángeles no es responsable del material visto, descargado o recibido por los usuarios a través de la Internet. Los sistemas de correo electrónico pueden presentar mensajes no solicitados con contenido ofensivo.

16.9 ACCESO A SERVIDORES

- El único personal que puede acceder al cuarto de servidores de la red y el sistema de información es el personal autorizado de la subgerencia de gestión de información, utilizando para tal fin la tarjeta electrónica de proximidad.
- Las personas no autorizadas que requieran ingresar al cuarto de servidores incluyendo, sin limitantes, contratistas de reparación de equipos, personal de servicios generales, mantenimiento de infraestructura o aseo, deben solicitar el ingreso a la subgerencia de gestión de información quien aprobara o negara el acceso, aclarando que en caso de aprobación, nunca se prestaran llaves ni tarjetas de proximidad, el acceso se hará con la supervisión de un trabajador autorizado.
- Cuando un trabajador autorizado para ingresar al cuarto de servidores finaliza su relación de trabajo con el Hospital Infantil Los Ángeles, todos los derechos de acceso al cuarto de servidores debe ser revocado inmediatamente, Solicitando la devolución de la tarjeta de proximidad.
- Los visitantes que no tengan que efectuar reparaciones a equipos del Hospital, o que no necesiten estar dentro del cuarto de servidores, no deben entrar en dichas áreas.
- El acceso a toda oficina, sala de computación y área de trabajo que contenga información sensible debe ser físicamente restringido para limitar el acceso a aquéllos que necesitan la información.

Elaboró: ALEXANDER ACOSTA Actualizó: ALEXANDER ACOSTA	Revisó :CARLINA DOMINGUEZ T.	Aprobó: DORIS SARASTY R.
--	------------------------------	--------------------------