POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SERVICIO SALUD ACONCAGUA

Elaborado por:	Revisado por:	Aprobado por:
Alejandro Ojeda Astudillo JEFE U. DESARROLLO Y SOPORTE TIC	**Miguel Bravo Burgos** Jefe Departamento TIC	Humberto Opazo Galaz SUBDIRECTOR DE RECURSOS FISICOS Y FINANCIEROS
Fecha: Marzo 2016	Fecha: Marzo 2016	Fecha: Marzo 2016

I. Introducción:

El Servicio de Salud Aconcagua, considera relevante las tecnologías de información y comunicaciones (TIC) para alcanzar sus objetivos institucionales. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

1. Objetivo

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Las TIC deben estar protegidas contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que el Servicio de Salud Aconcagua y su personal debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

2. Alcance:

Conforme la Misión de la Entidad, el Servicio de Salud Aconcagua estima la aplicación de la presente política de seguridad en todos los establecimientos de Red Asistencial que dependan directamente del Servicio de Salud.

3. Asignación de responsabilidades:

Las funciones del Comité de Seguridad Informática serán las siguientes:

- Aprobar los lineamientos de gestión de la seguridad de la información, en los establecimientos del Servicio de Salud Aconcagua, a través de compromisos.
- Revisar y aprobar las políticas de seguridad de la información que se propongan para el Servicio de Salud Aconcagua.
- Definir y establecer los roles y responsabilidades de las personas que tendrán a cargo la seguridad de la información en sus establecimientos.
- Conocer los riesgos a los cuales se encuentran expuestos los activos de la información.
- Revisar y analizar los incidentes de seguridad de la información.
- Aprobar iniciativas para mejorar la seguridad de los activos de la información.
- Definir las acciones a seguir en caso de situaciones no previstas que afecten la continuidad de los procesos críticos de la Institución.
- Aprobar las medidas a adoptar por el mal uso de los activos de la información del

Servicio de Salud Aconcagua, además de las contempladas en la Legislación vigente.

- Promover la gestión de la seguridad de la información dentro de la Institución.

El "Comité de Seguridad Informática", actualmente está conformado por los titulares de los siguientes cargos, según Resolución Exenta Nº 162 del 24/01/12, el cual será complementado de acuerdo a la nueva Norma Chilena ISO-27.0001 :

a. Subdirector Administrativo del Hospital San Camilo de San Felipe.
b. Subdirector Administrativo del Hospital San Juan de Dios de Los Andes.
c. Subdirector Administrativo del Hospital San Francisco de Llay-Llay.
d. Subdirector Administrativo del Hospital San Antonio de Putaendo.
e. Subdirector Administrativo del Hospital Psiquiátrico, Dr. Philippe Pinel de Putaendo
f. Jefe del Departamento TIC.
g. Encargado de Seguridad Informática del Servicio de Salud
h. Jefe Unidad de Soporte Informática del Hospital San Camilo
i. Jefe Unidad de Soporte Informática del Hospital San Juan de Dios
j. Jefe Unidad de Soporte Informática del Hospital San Francisco
k. Jefe Unidad de Soporte Informática del Hospital San Antonio
l. Jefe Unidad de Soporte Informática del Hospital Dr. Philippe Pinel

4. Desarrollo:

Prevención:

El Servicio de Salud Aconcagua debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar las medidas mínimas de seguridad determinadas por los especialistas y aprobadas por el Comité, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, el Servicio de Salud Aconcagua debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección:

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorear la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en la Norma Chilena ISO-27.0001.

El Monitoreo es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales

Respuesta:

El Servicio de Salud Aconcagua debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con el Servicio de Salud Aconcagua.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional: Iris-CERT, CCN- CERT, etc.

Recuperación:

Para garantizar la disponibilidad de los servicios críticos, el Servicio de Salud debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación

5. Registro de Información:

5.1 Políticas Generales

Sera Responsabilidad del comité de Seguridad la revisión anual de estas políticas y la propuesta de revisión y mantención de la misma.

Los funcionarios tienen conocimiento que los software utilizados por el Servicio de Salud son de uso interno y solo para realizar las tareas correspondientes a esta , y bajo ninguna circunstancia podrá:

- Reproducir, divulgar, transmitir o copiar, total o parcialmente, en medio magnético, escrito u otro cualquiera, los softwares utilizado por El Servicio de Salud Aconcagua, sin la autorización correspondiente.
- Prestar o facilitar el software utilizados por El Servicio de Salud Aconcagua, sin autorización correspondiente.
- Instalar o utilizar algún software no adquirido por El Servicio de Salud Aconcagua.
- Facilitar el uso de datos, entregar datos o reproducir total o parcialmente la información generada o utilizada en su trabajo a personas ajenas al Servicio de Salud Aconcagua o a personas del Servicio de Salud Aconcagua que no sean parte de los procesos administrativos correspondientes , sin autorización previa

- El Correo Electrónico, Internet e Intranet son de uso exclusivo para trabajos de la Institución y queda restringido el uso para otros fines o actividades contrarias a los intereses del Servicio de Salud Aconcagua

- Se prohíbe expresamente el acceso, bajada de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, videos, música, etc., o que atente contra las buenas costumbres o principios.

- Asimismo, "el Funcionario", será responsable por la incorporación de cualquier virus en el equipo computacional asignado a su cargo, esto necesariamente afectara el incumplimiento de las de las clausulas estipuladas en los párrafos anteriores.

5.2 Acceso a Internet:

Reducir el riesgo para el Servicio de Salud Aconcagua través de la implementación, de políticas y procesos de soporte que permitan identificar y bloquear el tráfico a Internet a sitios ajenos a las actividades que realiza el Servicio de Salud Aconcagua o peligrosos para la operación de la Institución. Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios para la institución y disminuir el riesgo de virus.

Esta política se aplicará a todo tráfico de navegación en Internet originado en cualquiera de las Redes del Servicio de Salud Aconcagua, y será obligatoria para todos los funcionamientos del servicio.

- El acceso a Internet e Intranet son de uso exclusivo para trabajos para el Servicio y queda restringido el uso para otros fines o actividades contrarias a las labores que se desempeñan en la Institución.
- Se prohíbe expresamente el acceso, bajada de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

- Todos los requerimientos de navegadores de Internet iniciados desde el servicio deberán ser filtrados para bloquear el acceso a sitios ajenos a las actividades que realiza negocio o tráfico innecesario.

- Todo Equipamiento Instalado en la institución , debe ser configurado para que pase por los mecanismos de filtrado dispuestos por la institución
- La configuración de bloqueo de sitios es: Acceso Full y Acceso Institucional, bloqueo general a sitios no autorizados.
- Todo acceso a los sitios pornográficos esta NEGADO.
- Todo acceso a sitios de juegos o apuestas esta NEGADO

5.3 Manejo de Archivos Impresos

Es muy importante tener presente las siguientes políticas para el manejo de impresiones de documentos:

- Las impresoras asignadas, solo podrán ser utilizadas para imprimir documentos correspondientes a las labores que realiza el Servicio de Salud Aconcagua.

- Cuando un usuario envíe un documento a una impresora Centralizada, debe tener muy presente el retirar su documento desde la impresora, ya que estos pueden tener información reservada para la institución.

- Todo documento que no sean retirados en un tiempo prudente desde una impresora centraliza, será eliminado.

- En caso de que un funcionario detecte un mal funcionamiento en una impresora, o que está siendo mal utilizada, deberá informar de inmediato al área de Soporte correspondiente a su establecimiento.

- El material impreso que contenga información delicada para la institución debe :

  - No dejarlo descuidado en áreas abiertas
  - Ser removido de las impresoras sin demora, ya que su información debe ser cautelada.
  - Si la información impresa es de carácter reservado, deberá almacenarse con la seguridad que corresponde.

5.4 Manejo Apropiado de Contraseñas

A continuación detallaremos las políticas existentes para la correcta utilización de cuentas y contraseñas de acceso a todos los sistemas del Servicio de Salud Aconcagua, adicionalmente podrá encontrar algunos consejos que permitirán definir buenas contraseñas.

Seguridad de la Contraseña

- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- Nunca compartas las contraseñas que se relacionan a tu usuario, y nunca le digas a nadie cual es. Inclusive el Jefe de Área no tiene el derecho de preguntar por tu contraseña.
- Cambia tu contraseña inmediatamente si piensas que alguien más la conoce, si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar o de trabajarlas.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido. Si lo haces inadvertidamente, sobre-escribe la contraseña guardada con una inválida y guárdala para remover la contraseña real. Alternativamente, cambia las contraseñas inmediatamente.
- Cambia tus contraseñas regularmente. En la mayoría de los sistemas se

recomienda que se cambien cada 30 días.

- Ten cuidado que no tengas personas observándote cuando ingreses tu contraseña.
- Conoce el procedimiento correcto a seguir si se te olvida la contraseña.
- No hay culpa ni penalidades por olvidar contraseñas. Es mejor que se te olvide la contraseña a que la escribas en algún lugar.
- No utilizar la opción de almacenar contraseñas en los exploradores de Internet

Cómo crear una contraseña buena y recordable

- Piensa en un tema que te interesa, y luego escoge palabras o frases que asocias con el tema.
- Para una contraseña más segura, piensa en dos palabras y utiliza parte de cada una.
- Contraseñas fuertes contienen números además de letras. Un ejemplo de contraseña para una persona que le guste pescar puede ser "vi3robalos".
- Tratar de utilizar las primeras letras de una frase. Por ejemplo "Yo tengo dos perros bien amistosos en casa" da la contraseña "yt2pbaec".
- No seleccionar cosas que otras personas saben de ti, por ejemplo: Nombre de un miembro de la familia. Patente del auto o Número de Teléfono.
- No utilizar palabras que pueden ser encontradas en un diccionario.
- No utilices siempre la misma contraseña con variaciones leves (ejemplo: "dejameentrar1","dejameentrar2").
- Trata de re-ingresar tu contraseña luego de uno o dos minutos de utilizarla.

Largo de la Contraseña

- Selecciona contraseñas que tengan por lo menos 8 caracteres de largo.
- Administradores deben utilizar contraseñas mucho más largas.
- La mayoría de los sistemas requieren un mínimo de largo para las contraseñas.
- Si son más de 8 caracteres, usualmente se debe a que el sistema o la información requiere controles de seguridad mayores.
- No utilizar el largo mínimo requerido. Mientras más larga la contraseña, más segura es.

Manejando Múltiples Contraseñas

- Considera utilizar la misma contraseña para más de un sistema.
- Trata de cambiar todas tus contraseñas siempre que tengas que cambiar una de ellas. Esto tiene dos beneficios:
  Menos tiempo se utiliza para cambiar contraseñas.
  Hacer que las contraseñas tengan relación entre sí hace que las puedas recordar con mayor facilidad.
- Si una computadora a la cual tienes acceso necesita cuidado especial, porque accede datos personales o es utilizada para autorizar pagos, utiliza una contraseña individual para esa computadora, y utiliza una contraseña común para otros sistemas. De esta manera solo tendrías que recordar 2 contraseñas distintas.

Puntos para Recordar

- Manteniendo las contraseñas seguras te protegerás a ti y la información a la cual tienes acceso. Nadie más puede entrar como si fueses tú si tu contraseña es un secreto bien guardado.
- La institución es dueña de toda la información creada bajo tu usuario y, aunque las Jefaturas no deben compartir tu usuario o contraseña, tienen la potestad de conseguir formalmente acceso a la información en cualquier momento.
- Si tus sistemas ofrecen la opción de "recordar" tu contraseña, o de llevar a cabo un "auto-logon", no habilites esas opciones.

Que debe contener una contraseña de red del SSA

- La contraseña debe poseer a lo menos una letra mayúscula.
- La contraseña debe poseer a lo menos una letra minúscula.
- La contraseña debe poseer a lo menos un número.
- El largo mínimo de la contraseña debe ser de 8 caracteres
- La contraseña no debe ser igual a ninguna de las últimas 13 contraseñas.
- La contraseña no debe corresponder solo a un cambio de número o letra. Ej de contraseña antigua: Pedrito01 - contraseña nueva: Pedrito02.

5.5 Políticas De Información y Toma de Conciencia

¿Cómo se informará?

La entrega de información a los usuarios es fundamental, pero esta información debe ser lo suficientemente clara y concreta para que el usuario la entienda y retenga con facilidad. Es a partir de este punto que se han definido los siguientes mecanismos de entrega de información.

- Correo a todos los usuarios: Este mecanismo se utilizará con el fin de entregar información muy importante y de rápida distribución. Ej. Alertas de nuevos Virus, cambios en los sistemas, cambios en procedimientos, etc.

- Publicación en la Intranet: Informaciones más extensas serán incorporadas en la Intranet, cabe señalar que por configuración de los equipos, al momento de que el usuario se conecta a su equipo, automáticamente le aparece la página principal de nuestra Intranet, en ella encontrara destacada la información y podrá leer con mayor detención.

- Charlas explicativas: estas actividades tienen la mayor complejidad pues obligan a coordinar a grupos de personas y mayor tiempo de preparación. Adicionalmente será muy complejo poder incorporar a todo el personal del establecimiento. Debido a lo anterior, este tipo de actividades se reservará para temas de gran importancia.
  Con el fin de asegurar que una mayor parte de la información llegue a la mayoría de los usuarios, se podrá mezclar los 2 primeros medios de difusión.

Cabe señalar que el correo y la Intranet han sido definidos como mecanismos de información oficial para la Institución, por lo que no es posible desconocer la información que a través de ellos es entregada.

¿Qué se informará?

La información que se entregue a través de cualquiera de los tres mecanismos antes señalados deberá ser oficial y por lo tanto deberá contar con la aprobación del Servicio de Salud Aconcagua.

La información que se entregará a los usuarios debe incluir consejos de buen uso de la información, claves, procedimientos ante virus, procedimientos de respaldo de la información, etc.

5.6 Control de Incidencias (Virus)

A continuación detallaremos las políticas de operación y control de virus Existentes en la Institución.

Objetivos

Reducir el riesgo para la El Servicio de Salud Aconcagua a través de la implementación, de políticas y procesos de soporte que permitan identificar y bloquear virus. Resguardando el correcto funcionamiento de los equipos computacionales.

Aplicación

El cumplimiento de esta política es obligatorio para todas las dependencias del Servicio de Salud Aconcagua. Y debe ser aplicada a todos los equipos que tengan instalado una versión de Antivirus.

Políticas de Uso

- Debe instalarse y desplegarse un software antivirus en todos los sistemas de información, (en los que se disponga de un software antivirus para el entorno del sistema operativo). Para El Servicio de Salud Aconcagua se ha definido como producto estándar Viruscan de McAfee, o el que determina el equipamiento MINSAL.

- Deben instalarse y desplegarse versiones actualizadas del software antivirus para permitir la detección y eliminación de virus en tiempo real, además de una verificación periódica en busca de virus, detección y reparación de los medios de almacenamiento de datos.

- El software antivirus que se haya instalado debe configurarse de modo que detecte y elimine, del modo más eficaz, el mayor número de posibles virus.

- La detección y eliminación de virus debe registrarse y dichos registros deben ser revisados por el equipo de Seguridad de TIC. Dentro del posible debe enviarse automáticamente un mensaje de alerta a las personas del equipo de Soporte del Establecimiento.

- Debe comunicarse de inmediato cualquier infección por virus al equipo de Seguridad de TI.

- Deben probarse nuevas versiones de software antivirus (incluyendo actualizaciones del motor de escaneado y archivos 'SuperDAT') en entornos controlados. Una vez que haya sido aprobado para su uso, el software deberá ser rápidamente desplegado a los usuarios. En situaciones de emergencia (por ejemplo, brotes importantes de virus), los periodos de prueba y despliegue se reducirán al mínimo razonable (este requisito no es aplicable a los nuevos archivos de definiciones de virus).

- Cuando se utilice un despliegue automático del software antivirus, deberá haber un sistema de respaldo para reinstalar la versión anterior del software en caso de que la nueva versión no funcione correctamente.

- Los soportes extraíbles serán escaneados antes de su uso, o lo antes posible si se utiliza como dispositivo de arranque (bootdisk).

- Un PC doméstico está sujeto a los mismos controles de seguridad que un PC de la institución, por lo que debe contar con un software antivirus actualizado.

- Los funcionarios no podrán bajo ninguna circunstancia desinstalar el producto de antivirus existente en su equipo.

- Los funcionarios, no podrán bajo ningún motivos instalar o reemplazar el antivirus que fue desplegado por la institución.

Qué hacer en caso de detectar virus

Si obtiene un mensaje de alerta al leer un archivo desde un medio magnético extraíble, desde un correo, o simplemente al navegar a través de internet presione el botón Limpiar del mensaje, si no es factible limpiar el archivo proceda a eliminarlo. Posteriormente informe al área de Soporte de su establecimiento para que se verifique que su equipo no este infectado.

5.7 Creación de Cuentas de Sistemas

Ambiente de Producción
Toda cuenta que se requiera modificar en los sistemas de producción deberá ser solicitada a la Unidad de Recursos Humanos o Unidad de Informática, solo con la autorización de estas unidades se procederá a realizar los cambios correspondientes.

Creación o Modificación de Cuentas
El procedimiento de creación o modificación se rige totalmente por lo antes señalado, debe ser canalizado a las Unidades mencionadas.

Las cuentas de sistemas en producción que son administrados por el departamento de Soporte y que deberán ser solicitadas de acuerdo a lo

informado previamente son las siguientes:

- Cuenta de Red: Esta cuenta corresponde a la que utilizará cada usuario para conectarse a su equipo PC y obtener recursos de la red de los establecimientos.
- Cuenta de Correo Red Minsal
- Cuenta en Sistema SSAMENU: Con esta cuenta el usuario tendrá acceso a los datos de los Sistemas del Servicio de Salud Aconcagua.

Eliminación de Cuentas
La eliminación de cuentas se realizará de acuerdo al procedimiento formal ya señalado, pero en situaciones especiales como despidos del personal, podrá ser enviado un correo por parte del Jefe de Recursos Humanos solicitando el bloqueo temporal de las cuentas del funcionario en cuestión, formalizando a la brevedad la entrega del correspondiente formulario.

5.8 Correo Electrónico

A continuación se detalla las políticas de filtrado de correos electrónicos existentes en el Servicio de Salud Aconcagua

El objetivo de ellas es reducir el riesgo para el servicio a través de la implementación, de políticas y procesos de soporte que permitan identificar y bloquear correos externos al trabajo o posibles correos hostiles. Permitiendo de esta manera aumentar la velocidad del tráfico.

Estas políticas serán aplicadas a todos los correos enviados por y hacia Servicio de Salud y su cumplimiento es obligatorio

Políticas de Uso

- El contenido de cada correo puede y será revisado por personal del Servicio, así como también por sistemas automáticos.

- El Correo Electrónico es de uso exclusivo para trabajos del Servicio de salud y queda restringido el uso para otros fines o actividades contrarias a los intereses del Servicio de Salud Aconcagua

- Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

Políticas de Configuración
Se debe bloquear el acceso a todas las cuentas externas POP3 o WebMail (a excepción del dominio redsalud.gov.cl)

· Será bloqueado todo correo que contenga:
Virus (incluyendo VBScript, worms, virus hoaxes, etc.)
- SPAM

- En correos entrantes archivos del tipo: ejecutables, sonidos, video, imágenes.
- Todos los documentos entrantes con las siguientes extensiones: *.PPS,
*.EML, *.VBS, *.VBS, *.SCR, *.COM, *.BAT, *.PIF, *.ZIP

Bloqueo de Correo

En caso de bloqueo de la cuenta de correo deberá ser informado al encargado de informática del establecimiento para que proceda al desbloque de la cuenta.
Se enviará el correo original al destinatario indicando que los archivos adjuntos han sido retenidos, estos correos deberán ser solicitados al área de Soporte, quien verificará que el correo no cumpla con alguna regla de exclusión y solicitara la posible liberación o posible bloqueo a la mesa de ayuda de la red Minsal.

5.9 Políticas para Seguridad de Acceso

A continuación se detalla las políticas de seguridad de Acceso a los bienes de información y dependencias de resguardos de la información existentes en el Servicio de Salud Aconcagua

El objetivo de ellas es reducir el riesgo para el servicio a través de la implementación, de políticas y procesos de soporte que permitan identificar el acceso a los bienes de información. Permitiendo de esta manera aumenta el resguardo de la información.

Estas políticas serán aplicadas a todos bienes de manejo de información y dependencias de resguardo de resguardo del procesamiento de información

Políticas

- Se deberá controlar el acceso de terceras partes a las instalaciones de procesamiento de información del servicio de salud Aconcagua.
- Ante la necesidad del acceso de una tercera parte a la información, se deberá realizar una evaluación del riesgo para determinar la implicancia que puede afectar la seguridad en la institución.
- Los controles y las implicancias detectadas se deberán definir en un contrato con las terceras partes.

Accesos

Tipos de Accesos:

El tipo de Acceso dado a una tercera parte es de especial importancia. Los riesgos otorgados a través de una conexión de red son diferentes a los riesgos que resultan de un acceso físico.

- Acceso físico

Se debe resguardar el ingreso no autorizado de personas que no pertenezcan a la institución, a las oficinas, salas de procesamiento de información, salas de comunicaciones, gabinetes de comunicación, gabinetes de Archivos Etc...

- Acceso lógico
  Se debe resguardar los accesos lógicos a la información, se debe procurar de mantener un control de las autorizaciones externas de ingreso a las base de datos de la institución, como así el ingreso a los sistemas de información del Servicio de Salud Aconcagua.

  Seguridad en los Contratos
  Los convenios que involucran el acceso de una tercera parte a las instalación eso bienes de procesamiento de información de la organización, deberán incluirse en los contratos o una referencia a las norma de seguridad de la institución

  Se deberán considerar los siguientes términos en los contratos

- Política General de la Seguridad de la Información
- Protección de los bienes , se incluyen
- Procedimientos para proteger los bienes de la institución sea la información y los software
- Procedimiento a seguir en caso de que ocurra algunos incidentes con los bienes (perdida de información, modificación etc.).
- Integridad y disponibilidad de los bienes
- Restricciones de copiado y divulgación de la información
- Derechos de propiedad intelectual
- Responsabilidad concerniente a la instalación y mantenimiento del hardware y software.

5.10 Clasificación y Control de Bienes.

Objetivo
Mantener una protección apropiada a los bienes de información que se encuentren en las instalaciones del servicio de Salud Aconcagua, para estos se deberán contabilizar los bienes de información importantes y asignarles un encargado que vele por la correcta seguridad de la información.

Responsabilidad
Se deben Identificar los dueños de todos los bienes de importancia y se deberán asignar las responsabilidades de manejar los controles apropiados para el acceso a los bienes. La responsabilidad final recae en el usuario al cual se le ha entregado el bien.

Del Inventario
Se deberá mantener e implementar un inventario de los bienes importantes asociados a cada sistema de información. Cada bien debe identificar claramente, documentar y acordar su propiedad, junto con su actual ubicación y usuario al cual fue asignado

Bienes a considerar

Bienes de Información:
- Base de datos y archivos de datos
- Documentación del Sistema
- Procedimientos de apoyo
- Planes de seguridad

Bienes de Software
- Software de Aplicación
- De Sistema
- Herramienta de desarrollo y utilitarios.

Bienes Físicos
- Equipos de Computación (monitores, Periféricos Etc.)
- Equipos de comunicación
- Medios Magnéticos
- Otros equipos técnicos

6. Normas y Referencias

El marco normativo se sustenta en lo siguiente

- Decreto Supremo N°83 del año 2004
- Norma Chilena de seguridad NCH2777
- Circular A18/12 del 4 de mayo de 2012
- Ordinario A22/N°3890 del 2016, MINSAL, Políticas de Seguridad de la Información.

7. Distribución

Establecimientos dependientes del Servicio de Salud Aconcagua.

8. Revisión

Comité de Seguridad de las TIC

Registro de Modificaciones

Revisión	Registro de Modificaciones		
Nº	**Detalle**	**Nº**	**Fecha**
01	Creación Política	1	2012
02	Difunde Política	Ord. Nº 2058	2012
03	Actualización Política	2	2013
04	Actualización Política	3	2016