SALUD
SECRETARÍA DE SALUD

GOBIERNO DEL
ESTADO DE CHIAPAS

INSTITUTO
DE SALUD

Políticas para el Uso y Seguridad de Tecnologías de la Información y Comunicaciones del Instituto de Salud

Versión 1.0

14 de Julio de 2017

CHIAPAS NOS UNE

Autorización

Con fundamento en el Artículo 14, Fracción XV del Reglamento Interior del Instituto de Salud, se expide **Políticas para el Uso y Seguridad de las Tecnologías de la Información y Comunicaciones del Instituto De Salud del Estado**, para contribuir al desarrollo de las actividades de los Servidores Públicos que integran su Estructura Orgánica.

Dr. Francisco Ortega Farrera
Secretario de Salud y Director General del Instituto de Salud

Validación Técnica

Dirección de Planeación y Desarrollo
Dr. Rafael de Jesús Domínguez Cortés

Área de Informática
Ing. Christian Rodolfo Núñez Gamas

Grupo de Trabajo

Dr. Rafael de Jesús Domínguez Cortés
Director de Planeación y Desarrollo

Desarrollo del documento

Ing. Christian Rodolfo Núñez Gamas
Jefe del Área de Informática

Ing. Elesban Hiram Ramírez Sánchez
Coordinador del Área de Informática

Integración del Documento

Lic. Luis Ernesto Aréchar Narváez
Jefe del Departamento de Desarrollo Organizacional

Índice

Introducción

Este documento es publicado por la Dirección de Planeación y Desarrollo a través del Área de Informática del Instituto de Salud en la página de dicha Dirección General en la URL: http://www.salud.chiapas.gob.mx/doc/politicas_tics.pdf. Las políticas y lineamientos aplican para todas las áreas de Tecnologías de la Información del Instituto de Salud del Estado de Chiapas, incluyendo el personal bajo contrato por tiempo determinado, los proveedores y todos los sistemas informáticos y de comunicaciones utilizados por los servidores públicos del Instituto de Salud.

Estos sistemas incluyen las redes de área local, las computadoras personales (PC) y demás sistemas administrativos, los centros de telecomunicaciones y de conmutación, los proveedores de servicios de Internet (ISP) y otros proveedores externos de servicios de información.

Para el seguimiento y la correcta aplicación de este documento para beneficio del Instituto de Salud, a través de buenas prácticas, las cuales se determinan a través de dos puntos:

I. **Políticas de Uso de las Tecnologías de Información y Comunicaciones**
II. **Políticas de Seguridad de los Sistemas Informáticos y de Comunicaciones**

I. POLÍTICAS DE USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

1. PROPÓSITO

Definir políticas sobre el uso apropiado de los recursos informáticos disponibles en el Instituto de Salud del Estado de Chiapas.

2. ALCANCES

Este reglamento se aplicará a todo el personal que labora permanentemente y eventual en el Instituto de Salud, que tenga acceso a los recursos informáticos asignados por los titulares de las áreas.

También se aplica a todos los equipos y sistemas informáticos que el Sistema haya dispuesto para la ejecución de labores y para el propio desempeño de (servidores, equipos PC, laptops, equipos de comunicaciones, bases de datos, aplicaciones que apoyen los procesos sistemáticos, software licenciado, impresoras, periféricos e información electrónica) que se encuentren bajo responsabilidad operacional del Instituto de Salud.

3. TÉRMINOS/DEFINICIONES

Para los propósitos de esta política se aplicarán las siguientes definiciones:

Recursos informáticos: incluyen todo equipo informático hubs, accesspoint, cableado de datos) , software (desarrollo, gráfico, diseño web, administración de dominio, administración de base de datos ,seguridad de red, antivirus), aplicación y sistemas desarrollados para uso del Instituto de Salud, servicios (correo electrónico,

sitio web, base de datos bibliográficas), documentos electrónicos generados (word, excel, powerpoint, access, pdf, etc.) e información contenida en los sistemas de información.

Usuario: Es todo personal administrativo, profesional de la salud o cualquier otra persona no necesariamente vinculada con el Instituto de Salud que hace uso de un recurso informático interno. Todo único usuario asignado a un recurso informático se convierte automáticamente en custodio sin necesidad de documento de por medio.

Custodio: Es todo personal al cual se le ha asignado un recurso informático formalmente por documento, y que no necesariamente hace uso directo del mismo.

Material no autorizado: incluye la transmisión, distribución o almacenamiento de todo material que viole este Reglamento. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.

Red de Datos: es el conjunto de recursos informáticos que permite la comunicación de datos e información a través de todo el Instituto de Salud incluyendo el Internet.

Red: incluye cualquier sistema de cableado o equipos físicos como routers, switches, módems, sistemas de datos, voz y dispositivos de almacenamiento.

Sistemas de información: incluye cualquier sistema o aplicación de software que sea administrado y responsable por el Área de Tecnologías de Información y Comunicaciones del Instituto de Salud.

4. GENERALIDADES

El Instituto de Salud del Estado de Chiapas asigna al personal, a través del Área de Tecnologías de Información y Comunicaciones del Instituto de Salud, los equipos y sistemas de información básicos necesarios para la ejecución de las actividades laborales, en la medida de la disponibilidad de los mismos y con la aprobación

de las autoridad respectiva, convirtiéndose estas personas en usuarios, responsables por y custodios de estos recursos.

El acceso a los equipos y sistemas de información del Instituto de Salud es un privilegio y tiene por objetivo brindar facilidades para cumplir con los fines de servicio y laborales de cada área o ambiente en los que se asignaron.

Cada usuario tiene el deber de: respetar y custodiar la integridad de los equipos informáticos asignados, cumplir las licencias y acuerdos relacionado con los software adquiridos e instalados y las aplicaciones internas desarrolladas, así como actuar según políticas implementadas en este documento .

Las violaciones a las políticas y disposiciones establecidas en este reglamento con respecto al uso, operatividad y disponibilidad de los recursos informáticos, puede originar en la restricción o prohibición del acceso a los equipos y sistemas de información asignados u otras acciones disciplinarias o legales por parte del Instituto de Salud.

El Área de Tecnologías de Información y Comunicaciones del Instituto de Saludno asume responsabilidad alguna por el mal uso de los recursos informáticos asignados a los usuarios, sin embargo como responsable solidario de los equipos y sistemas de información, puede disponer de la información generada en ellos para apoyar las acciones disciplinarias y legales que crea convenientes en caso que se vea afectada por acciones de desprestigio por parte de los usuarios.

Aceptar cualquier cuenta o utilizar cualquier sistema de información constituye la aceptación de esta política por parte de los usuarios, aún desconociendo este reglamento, por tal motivo se solicita a los usuarios de estos recursos el respeto y colaboración para el cumplimiento de las normas que a continuación se enuncian.

5. POLÍTICAS Y NORMAS

A. SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS

El uso de los recursos informáticos (equipos, software, aplicaciones y sistemas, bases de datos, periféricos, documentos e información) es para asuntos relacionados con las labores relacionadas con el Instituto de Salud y con la actividad laboral para el que fue

Es responsabilidad de los usuarios mantener sus equipos de cómputo, disquetes y dispositivos USB libres de cualquier software malicioso (virus, troyanos, gusanos, adware, spyware, dialers, keyloggers, rootkits o PUPs - PotentiallyUnwantedPrograms). Así mismo, no está permitido el uso de los equipos informáticos, servicios y red de datos para propagar cualquier software malicioso de forma premeditada, esto será reportado al área pertinente del Instituto de Salud para que inicie las acciones a que haya lugar.

No está permitido provocar deliberadamente el mal funcionamiento de los bienes informáticos, redes y sistemas, propiedad del Instituto.

B. SOBRE LA INTEGRIDAD DE LOS RECURSOS INFORMÁTICOS

Se considera que el usuario está incurriendo en falta grave por negligencia, cuando destruye o daña los equipos informáticos que se le hayan asignado para realizar su labor o actividad o cuando manipula cualquier otro equipo del Instituto de Salud que no es de su uso normal.

Está prohibido manipular comidas, bebidas o fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterior del mismo, en estos casos se informará vía documento al área pertinente del Instituto de Salud para que ésta determine las acciones a seguir o el remplazo del equipo por parte del usuario.

No está permitida la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos de cómputo, equipos de comunicaciones, la estructura de red, las aplicaciones desarrolladas, la base de datos, el servicio de internet, el correo electrónico y los servicios y/o recursos informáticos asociados.

Se prohíbe intercambiar dispositivos (monitores, teclado, mouse, no break, reguladores) de una computadora a otra.

Se prohíbe cambiar de ubicación los equipos de cómputo, el personal del Área de Tecnologías de Información y Comunicaciones del Instituto de Salud es el único autorizado para

realizar dicha tarea; En caso de que requiera sacar de las oficinas del Instituto de Salud cualquier bien informático, deberá solicitar autorización al Área de Tecnologías de Información y Comunicaciones del Instituto de Salud.

En caso de que algún equipo (propiedad del Instituto de Salud, en comodoto, o particular autorizado) presente alguna falla o anomalía, deberá reportarla por escrito al Área de Tecnologías de Información y Comunicaciones del Instituto de Salud. El personal del Área de Tecnologías de Información y Comunicaciones del Instituto de Salud es el único autorizado para inspeccionar y dar mantenimiento los equipos. La intervención de terceros en la inspección o mantenimiento de los bienes informáticos está prohibida y es bajo la estricta responsabilidad del usuario.

C. SOBRE EL ACCESO A LA RED DE DATOS

La cuenta y la contraseña de acceso a la Red de Datos, al Correo, a Intranet, a los Sistemas de cómputo, y otros que se creen por el Área de Tecnologías de Información y Comunicaciones del Instituto de Salud, son de la propiedad del Instituto de Salud, y son para uso estrictamente personal y se encuentran bajo responsabilidad del usuario al que se le asigna dicha cuenta.

El acceso a la red de datos y a los servicios de información debe hacerse desde un equipo debidamente registrado y/o autorizado por el Área de Tecnologías de Información y Comunicaciones del Instituto de Salud. Este equipo debe disponer de un nombre de maquina registrado en el DNS del Servidor de Dominio y una dirección IP dentro del rango de números IP legítimos definidos por la Unidad de Informática para uso interno del Instituto de Salud.

No está permitido el acceso desde cualquier equipo y sistemas de información para obtener información o archivos de otros usuarios sin su permiso o para acceder a información que no es de su área o competencia, salvo requerimiento por escrito de su jefe área inmediato o por decisión de las autoridades del Instituto de Salud.

No se deberá usar cuentas y contraseñas ajenas a las asignadas inicialmente al usuario por el personal de la Unidad de Informática. Así mismo es responsabilidad de los usuarios no facilitar a ningún otro su cuenta y su contraseña personal, que puede

designado, siendo el uso personal limitado.

El empleo de los recursos informáticos de forma no indicado expresamente por documento al titular del Área de Tecnologías de Información y Comunicaciones del Instituto de Salud, a través de los titulares de las áreas, se encuentra por defecto terminantemente prohibido. Los usuarios se limitarán a trabajar con los recursos informáticos asignados y en caso de requerir más recursos deberán solicitarlos a través de su titular de área.

El uso personal de los equipos, software, servicios y periféricos, es permitido al usuario para actividades laborables no comerciales, siempre y cuando esté autorizada debidamente, acate las políticas implementadas en este documento, no interfiera con las actividades operativas normales del Instituto de Salud, no afecten a los demás usuarios y no influyan negativamente en el desempeño de tareas y responsabilidades asignadas al puesto, en caso contrario debe ser negado.

El uso de equipos particulares deberá contar con la autorización por escrito del superior jerárquico inmediato y deberá ser informado al Área de Tecnologías de Información y Comunicaciones del Instituto de Salud.

No está permitido imprimir trabajos personales sin autorización del titular del área o empleando los recursos del área (papel, tóner, tinta, cinta).

No deberá usar los recursos informáticos para acceso, descarga, transmisión, distribución o almacenamiento de material: obsceno, ilegal, nocivo o que contenga derecho de autor, para fines ilegales.

No está permitido el uso de los recursos informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros. En el caso de las Jurisdicciones o Centros de Salud queda bajo la responsabilidad de sus titulares velar por el cumplimiento de esta política.

En las oficinas: los equipos de cómputo, los software y aplicaciones instalados en ellos, son usados únicamente por el usuario asignado o por las personas designadas por el uso de dichos equipos.

No está permitido usar los equipos informáticos incluidas las impresoras del Instituto de Salud para fines que no sean propias de la labor del usuario.

derivar en robo de información o manipulación de los documentos electrónicos, en los equipos informáticos, salvo que por necesidad de reparación el personal de la Unidad de Informática los requiera para reconstruir su perfil y documentación en el equipo dañado. En este caso el usuario posteriormente tiene el derecho de solicitar el cambio de su contraseña.

No se permitirá ningún intento de vulnerar o atentar contra los sistemas de protección o seguridad de red. Cualquier acción de este tipo será comunicada inmediatamente al área pertinente del Instituto de Salud para que ésta pueda iniciar cualquier acción de carácter administrativo, laboral o legal que corresponda.

No está autorizada la descarga y distribución de archivos de música, videos y similares con fines no laborables.

No está autorizada la instalación de puntos de acceso inalámbricos (accesspoint - wifi) que se encuentren fuera de la administración (configuración y supervisión) de la Unidad de Informática, porque implican una brecha de seguridad a la información que se maneja dentro del Instituto de Salud.

No están autorizadas las acciones de usuarios, o terceras personas que estén destinadas a modificar, reubicar o sustraer los equipos de cómputo, software, información o periféricos para alterar o falsificar de manera fraudulenta su contenido.

El usuario no deberá acceder a los sistemas de información, servicios y bases de datos para los cuales no se le ha otorgado expresamente permiso, ni imprimir información confidencial y sacarla fuera de los ambientes del Instituto de Salud con la finalidad de publicarla o manipularla para perjudicar el funcionamiento de la institución.

Los accesos a los diferentes sistemas de información por los usuarios deberán ser solicitados vía documentación escrita elaborada por su respectivo titular de área y dirigido al Jefe de la Unidad de Informática. Se evaluará si el requerimiento es justificable y acorde

a la actividad que realiza el solicitante, recomendando por documento o comunicación verbal.

El término de la relación laboral con la institución le faculta al Jefe de la Unidad de Informática inhabilitar inmediatamente la cuenta de usuario y/o modificar la contraseña actual, y transferir toda la información que haya creado durante su periodo laboral al personal designado y reconocido por el titular de dicha área, previa comunicación escrita dirigida al Secretario del Instituto de Salud.

D. SOBRE LA INSTALACIÓN Y USO DE SOFTWARE Y APLICACIONES

El software y las aplicaciones que serán instalados en los equipos informáticos serán aquellos que previamente hayan sido estandarizados por la Unidad de Informática y/o autorizado por la oficina del C. Secretario del Instituto de Salud, para lo cual se dispone de las licencias respectivas.

No deberá instalarse ningún tipo de software que no se encuentre autorizado por la Unidad de Informática ni licenciado por la oficina del C. Secretario del Instituto de Salud en los equipos informáticos. El usuario es el responsable ante el Instituto de Salud y/o ante terceros por la instalación y uso de cualquier software no autorizado que haya sido colocado en el equipo informático de su uso.

No está permitido desinstalar software, aplicaciones, borrar archivos del sistema o cambiar configuraciones pre-establecidas para los equipos informáticos sin supervisión o conocimiento del personal de la Unidad de Informática.

No está autorizada la copia o distribución, para fines personales o comerciales, de cualquier aplicación o software protegido legalmente o violar cualquier derecho de autor o términos de licenciamiento adquiridos por el Instituto de Salud, sin la autorización escrita del propietario del software.

No está permitido la instalación o uso de software de espionaje, monitoreo de tráfico o programas maliciosos en la red de datos que originen: violaciones a la seguridad, interrupciones de la comunicación en red, que eviten o intercepten la autenticación del usuario (inicio de sesión en el dominio) por cualquier método, o que busquen acceder a recursos a los que no se les ha permitido

expresamente el acceso.

Toda instalación, desinstalación o traslado de software incluyendo los de "dominio público" o de "distribución libre desde y hacia un equipo informático" del Instituto de Salud, requiere autorización y coordinación previa con la Unidad de Informática.

El usuario es consciente y reconoce los derechos del Instituto de Salud al usar una licencia de software adquirido por la institución en un equipo informático del Instituto de Salud o en un equipo de cómputo personal.

Cualquier software o aplicación instalado en un equipo informático que no cumpla con lo estipulado anteriormente, será desinstalado sin aviso previo y sin que ello origine ninguna responsabilidad del personal de la Unidad de Informática.

E. SOBRE EL USO DEL CORREO ELECTRÓNICO

Está prohibido usar los equipos de cómputo del Instituto de Salud para enviar mensajes de amenaza o acoso a los usuarios de la institución o externos, lo cual será comunicado a las autoridades correspondientes para la sanción inmediata del usuario y el seguimiento respectivo de la Unidad de Informática.

No está permitido el envió de correos de tipo spam o con comunicaciones fraudulentas desde las cuentas institucionales, que originen daños a la imagen del Instituto de Salud; tampoco está permitido remitir correos con mensajes, imágenes o videos obscenos o inmorales desde o hacia el Instituto de Salud.

No está permitido usar identidades falsas en mensajes de correo electrónico institucionales, ya sea con direcciones ficticias o con una identidad que no sea la propia asignada por la Unidad de Informática del Instituto de Salud (cuenta de correo personal).

No está permitido usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores, revelar información privada sin el permiso explícito del dueño, dañar o perjudicar de alguna manera los recursos disponibles electrónicamente, para apropiarse de los documentos de la facultad.

Todas las políticas incluidas en este documento son aplicables al correo electrónico institucional. El correo electrónico debe usarse de manera profesional y cuidadosa, tomando especial cuidado en evitar el envío a destinatarios dudosos ó destinatarios colectivos. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.

No es aceptable el uso de correo institucional para participar en una cadena de correos, se recomienda borrar este tipo de mensajes en el momento de recepcionarlo.

En ningún caso es permitido suplantar cuentas de usuarios ajenos.

F. SOBRE EL ACCESO A INTERNET Y OTROS SERVICIOS WEB

El usuario es responsable del uso del servicio de navegación en internet.

No está permitido el uso indebido de los recursos de internet con fines personales no laborables.

Está restringido el uso de páginas sin fines de investigación que no se relacionen con el área de trabajo.

Los usuarios con servicio de internet deberán utilizarlo única y exclusivamente para la consulta, estudio, análisis y manejo de información relacionada a las funciones y actividades que desempeña. NO debe utilizarlo para acceso a páginas de descarga de música, películas, series, software no autorizado, imágenes ofensivas o con relación a cuestiones raciales, creencias religiosas o políticas y de pornografía en cualquier modalidad (juegos, chistes, video, audio, etc.).

No está permitido acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real).

No es permitido el uso de dispositivos particulares de acceso a Internet, de tipo banda ancha móvil, sin la autorización por escrito del superior jerárquico inmediato y deberá ser notificado a la Unidad de Informática.

No está permitido usar cualquier tipo de conversación en línea,

sin el requerimiento respecto y/o el permiso expreso de las autoridades.

No está permitido degradar el ancho de banda de la conexión de Internet, debido a descargas de archivos de música, imágenes, videos, etc. o empleo de radio o video en línea, no autorizado.

Queda restringido el uso de programas peer to peer (p2p) para el intercambio de archivos.

No está permitido degradar el ancho de banda de la conexión de Internet, a través de la instalación de software que intente o logre vulnerar el Firewall; ejemplo de este puede ser el UltraSurf.

El titular Área de Tecnologías de la Información y de Comunicaciones del Instituto de Salud, internet acogiendo las directivas del Instituto de Salud determinará los estándares para los contenidos considerados como oficiales para uso laboral, así como los necesarios para su desempeño. Cualquier otra página o sitio web puede ser bloqueado sin necesidad de comunicación al usuario.

El titular del Área de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud, administrará los servicios de mensajería instantánea (Chat, MSN, Yahoo Messenger, ICQ, IRC), redes sociales (Facebook, Twitter), entre otros, telnet, FTP, SSH, en apoyo a las labores de las áreas de trabajo.

El encargado o encargada del diseño y/o mantenimiento del sitio web o WEBMASTER, que manipule información referente al Instituto de Salud debe acogerse a las políticas del Instituto de Salud del Estado de Chiapas incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software. El contenido debe ser revisado periódicamente para asegurar su veracidad.

G. SOBRE LA PRIVACIDAD DEL USUARIO DE LOS RECURSOS INFORMÁTICOS

Cuando los equipos y sistemas informáticos funcionan correctamente, el usuario puede considerar que los datos generados en estos, son información privada, al menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios

deben estar conscientes sin embargo, que ningún sistema de información es completamente seguro, y que hay personas dentro y fuera del Instituto de Salud que pueden encontrar formas de tener acceso a la información.

El personal de soporte técnico tiene la autoridad para acceder archivos individuales o datos cada vez que deban realizar mantenimiento, reparación o chequeo de equipos de computación, también tiene la facultad de eliminar archivos innecesarios que degradan el buen funcionamiento del equipo y que no estén autorizados (software no autorizado, archivos de música y video).

Cuando se sospeche de uso indebido de los recursos informáticos, el personal de la Unidad de Informática, con la autorización respectiva puede acceder a cualquier cuenta, datos, archivos, o servicio de información perteneciente al usuario involucrado para investigar e informar a los directivos del Instituto de Salud respectivos.

El personal del Unidad de Informática está autorizado a monitorear los sistemas de información del Instituto de Salud para salvaguardar la integridad, disponibilidad, seguridad y desempeño correcto de los mismos y ejecutar las acciones pertinentes como: negación, restricción de acceso de usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

El personal de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud administrará y optimizará los recursos del servicio de internet que sean proporcionados.

El personal de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud implementará las herramientas que permitan el monitoreo las cuales posibilite analizar y detectar el uso indebido del servicio.

El personal de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud, procederá a la suspensión del servicio de internet a los usuarios que lo utilicen con fines no relacionados a sus labores.

El personal de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud, se verá obligado a la elaboración de un reporte administrativo, habiendo verificado el incumplimiento de las políticas que a continuación se mencionan.

El personal de Tecnologías de la Información y de Comunicaciones del Instituto de Salud del Instituto de Salud monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes, recolectando estadísticas de utilización basado en las direcciones de red, protocolo de red y tipo de aplicación, restringiendo las actividades del usuario y el uso de las aplicaciones innecesarias cuyo uso resulte en la degradación del rendimiento del tráfico y se informará a la autoridad respectiva.

6. SOBRE EL USO RACIONAL DE LOS RECURSOS

El usuario, antes de imprimir un documento deberá revisar la opción "vista preliminar" y revisar el formato del documento para que no tenga que repetir la impresión.

El personal del Instituto de Salud deberá acatar en todo momento el Decreto de Austeridad, Disciplina y Racionalidad del Gasto.

II. POLÍTICA DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

1. Principios Generales

El acceso a los sistemas e información importante debe estar restringido al personal autorizado, justificarse por requisitos y debe registrar identidad de usuarios.

Debe controlarse el acceso al sistema por medio de identidades de usuario y contraseñas secretas asignadas a usuarios autorizados.

El software de seguridad debe estar adecuadamente protegido contra acceso o modificaciones no autorizadas.

Esta norma aplica al acceso del personal de la DGSEI a todos los tipos de sistemas y aplicaciones internas del mismo, incluyendo equipos de telecomunicación de información y voz, servidores, las PC y otras estaciones de trabajo.

2. Responsabilidades y División de Deberes

Se debe garantizar que:

a) las responsabilidades para la administración de controles de acceso al sistema estén separadas de otros deberes incompatibles si dicha situación debilitaría de manera inaceptable los controles de seguridad.

a) Algunos ejemplos de dichos deberes incluyen la operación de sistemas, el soporte técnico, el desarrollo de sistemas y la utilización para fines de la organización;

b) se documenten todas las solicitudes para crear, cambiar o borrar los derechos de un usuario de sistema, y que dichos procedimientos cuenten con la autorización de la administración de usuarios, y de ser necesario, la de otras responsables por la información de los sistemas que concierne, guardando dicha documentación como referencia durante por lo menos 6 meses;

c) los procedimientos hagan cumplir los controles adicionales de los requisitos que representen un alto riesgo particular, tales como el mantenimiento del equipo y las contraseñas creadas para usarse

una sola vez para la resolución de problemas del sistema de producción;

d) los detalles de las identidades y contraseñas de usuario sean distribuidas a los usuarios del sistema a través de medios seguros;

e) los derechos de acceso al sistema sean revisados con regularidad y cancelados cuando el usuario ya no los requiera. Debe asignarse un responsable específico para la revisión y mantenimiento de contraseñas;

f) los procesos administrativos sean supervisados para asegurarse de que los controles sean adecuados en relación con el riesgo, y sean operados de forma correcta y coherente.

3. Identidades de Usuarios

Las identidades de usuario deben:

a) identificar de forma única a un usuario individual;

b) evitar identificar los derechos de acceso al sistema específicos otorgados a un usuario, ni proporcionar información alguna acerca de la contraseña del usuario o los sistemas concernientes. En casos excepcionales, la Dirección puede autorizar identidades genéricas para identificar a grupos bien definidos de usuarios para fines específicos.

4. Contraseñas

Las contraseñas deben contar al menos con 8 caracteres imprimibles sin espacios. Las contraseñas deben construirse considerando lo siguiente:

a) Debe contener letras mayúsculas y minúsculas.

b) Debe contener números y caracteres de puntuación 0-9, !@#$%^&*()_+|~-

=\`{}[]:";'<>?,./)

Las contraseñas no deben ser fácilmente predecibles o adivinables, y en particular no deben ser fácilmente asociadas con el usuario, tales como:

a) nombres o iniciales;

b) nombres, códigos de identificación o referencias de su compañía;

c) número de placas de automóviles;

d) meses del año, días de la semana u otros criterios de fecha;

e) números de teléfono;

f) identidad de usuario, nombre de usuario, identidad de grupo o código identificador de sistema.

Todas las contraseñas a nivel sistema (root, administrador, enable y cualquier cuenta con privilegios de administración) deberán cambiarse al menos cada tres meses.

Cualquier tipo de contraseñas de usuario (email, web, computadora personal) deberán cambiarse al menos cada cuatro meses.

Las contraseñas no se comparten.

Las contraseñas no se deberán insertar en mensajes de correo electrónico u otro medio de comunicación electrónica.

Siempre que sea posible se aplicarán herramientas automatizadas según se considere apropiado para monitorear el cumplimiento de las contraseñas con la norma anterior.

5. Sistemas de Control de Acceso

Siempre que sea posible, los sistemas de control de acceso deben:

a) Hacer cumplir automáticamente la norma sobre contraseñas establecida en el punto 9.4 anterior;

b) Almacenar las contraseñas cifrándolas una sola vez para evitar que sean fácilmente descubiertas. Si las contraseñas son distribuidas de forma electrónica a lo largo de las redes, las mismas deben ser cifradas cuando se posible;

c) Habilitar a los usuarios para que cambien sus propias contraseñas, previa introducción de su contraseña actual. Debe solicitárseles que lo hagan inmediatamente después de recibir su contraseña inicial o cuando se emita una nueva contraseña, y de ahí en adelante al menos cada 90 días transcurridos. Debe tomarse en consideración un cambio más frecuente de contraseña, incluyendo las "contraseñas para utilizarse sólo una vez", en el caso de aplicaciones particularmente delicadas, tales como los

sistemas de pago o nómina y el acceso para resolución de problemas a los sistemas de producción. Si en circunstancias excepcionales se autorizan contraseñas compartidas, éstas deben ser cambiadas con prontitud tras su emisión inicial y siempre que uno de los usuarios no cuente más con autorización para su uso;

d) evitar que los usuarios seleccionen nuevamente contraseñas que hayan utilizado recientemente para garantizar un grado razonable de cambio regular;

e) desplegar un aviso que advierta ("banner de inicio de sesión") que el sistema sólo losusuarios autorizados pueden acceder al sistema, y que cualquier acceso no autorizado podría ser considerado como un acto criminal;

f) evitar desplegar las contraseñas o cualquier otra información que pudiera servir de ayuda para acceder sin autorización a terminales de computadoras o impresoras. Las contraseñas no deben ser registradas en pistas o registros de auditoria;

g) terminar la sesión y suspender los derechos de acceso del usuario tras tres intentos fallidos consecutivos de inicio de sesión, si no se logra un inicio de sesión en el tiempo máximo establecido, o si la terminal permanece inactiva durante un periodo de tiempo predeterminado;

h) suspender los derechos de acceso del usuario que no hayan sido utilizados durante un periodo de 90 días consecutivos. Posteriormente, las cuentas de usuarios suspendidos deben ser borradas tras 90 días de inactividad;

i) registrar una pista de auditoria de todos los intentos fallidos de inicio de sesión en sistemas significativos identificados con base en la evaluación de riesgo;

j) terminar la sesión de las terminales si las mismas permanecen inactivas por más de tiempo del estipulado como tiempo máximo. Cuando esto no sea posible, implementar protectores de pantalla protegidos con contraseña.

6. Instalación y Mantenimiento de Contraseñas

Las contraseñas iniciales provistas por los vendedores de equipos y software para propósitos de instalación, mantenimiento e ingeniería

son por lo regular muy bien conocidas y poderosas. Se las debe cambiar y desactivar cuando no se les requiera más.

7. Utilización de Identidades y Periodos de Tiempo Determinados de Terminal

Cuando sea posible la utilización de las funciones de sistemas críticos debe restringirse a terminales, impresoras y otros dispositivos de usuarios o departamentales designados, y limitarse a las horas y días especificados.

El desglose de las dos políticas antes señaladas serán observadas a través de los siguientes puntos:

INCUMPLIMIENTO DE LAS POLÍTICAS

El Instituto de Salud hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento. El Instituto de Salud se reserva el derecho de evaluar periódicamente el cumplimiento de este reglamento.

Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por el Instituto de Salud y en estricto acato a los Directivos y reglamento interno del Instituto de Salud.

El usuario que no cumpla con el uso correcto del software será directamente responsable de las sanciones legales derivadas de sus propios actos y de los costos y gastos en que pudiera incurrir el Instituto de Salud en defensa por el uso no autorizado o indebido de licencias de software.

APLICACIÓN Y CUMPLIMIENTO

Esta política aplica a todos los empleados del Instituto de Salud. Cualquier usuario que viole este reglamento será objeto de sanción disciplinaria pertinente, sea su relación de cualquier tipo laboral.

SANCIONES

El o los servidores públicos que dejen de cumplir con lo anteriormente mencionado, serán sancionados conforme a lo indicado en el Título Tercero, Capítulo Segundo, de la Ley de Responsabilidades de los Servidores Públicos del Estado de Chiapas, sin prejuicio de sanción que le imponga el Título Décimo Quinto, Capítulo Segundo de la Legislación Penal del Estado, publicados para su consulta en la página http://www.poderjudicialchiapas.gob.mx/Pagina/legislacion.php; además de las disposiciones legales aplicables.