SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Secretaría de Salud del Estado de Chihuahua

STI-POL-001 POLITÍCA DE SEGURIDAD DE LA INFORMACIÓN

Vigencia al 01 octubre 2024

Índice

1. Objetivo.

El objetivo principal de la presente política de alto nivel es, definir los principios y las reglas básicas para la gestión de la seguridad de la información. Con el fin de lograr que la Secretaría de Salud y sus Órganos Descentralizados garanticen la seguridad de la información y minimicen los riesgos derivados de un impacto provocado por una gestión ineficaz de la misma.

2. Alcance.

La Política es aplicable para todo el personal afiliado a la Secretaría de Salud y sus Órganos Descentralizados, que deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible.

Abarca toda la información de la Secretaría de Salud y sus Órganos Descentralizados, con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

3. Vigencia.

Esta política está vigente hasta el 01 de octubre del 2024

4. Responsabilidades.

Los responsables del funcionamiento adecuado para que se cumpla las Políticas de seguridad del organismo, se describirán a continuación;

Coordinador del Grupo Estratégico de Seguridad de la Información: Responsable de promover y aplicar el cumplimiento descrito en este documento, revisar y aprobar los cambios procedentes de actualizaciones.

Líder de Implementación: Impulsar al grupo de trabajo realizar los procedimientos que competen a cada uno de los integrantes del grupo estratégico de seguridad de la información.

Responsable de Aplicaciones: Proporcionar los procedimientos necesarios para la gestión, mejora y cumplimiento de las políticas de seguridad de la información de las aplicaciones.

Administrador de Bases de Datos (DBA): Responsable de dar soporte, gestionar, mantener la integridad y seguridad de la información de los datos de las diferentes aplicaciones.

Ingeniero de Red. Garantizar la seguridad en los sistemas de redes y telecomunicaciones, así como en la infraestructura, cableado, protocolos, herramientas de administración y seguridad de la red, realizar pruebas de conectividad entre los dispositivos de red, equipos clientes, Data center de Oficinas Centrales y Data Center del Hospital Infantil de Especialidades de Chihuahua.

Desarrollador de Aplicaciones: Responsable de diseñar, crear y mantener las aplicaciones de la Secretaría de Salud y sus Órganos Descentralizados, cumpliendo con las políticas de seguridad de la información descritas en este documento.

Administrador DATA CENTER: Administración, almacenamiento, respaldo, recuperación de información y soluciones de seguridad de los servidores virtuales de Secretaría de Salud y de sus

Órganos Descentralizados; así como monitorear que los servicios se encuentren activos, para el buen funcionamiento de las aplicaciones y sistemas.

Ing. Soporte: Instalación, mantenimiento, configuración de hardware y software en la institución para dar cumplimiento a la seguridad de la información.

5. Cumplimiento de normativa.

La presente política responde a las recomendaciones de la NOM-024-SSA3-2012 Sistemas de información de registro electrónico para la salud. Intercambio de información en salud, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas en el ámbito de la seguridad de la información.

6. Autorización.

Las políticas mencionadas son autorizadas por el Coordinador del Grupo Estratégico de Seguridad en la Información, en donde se contemplan los siguientes puntos;

a) Revisar y aprobar las políticas de seguridad de la información.
b) Identificar, analizar cambios y actualizaciones de las políticas, según sean las necesidades del organismo.
c) Seguimiento, control de riesgos y necesidades procedentes por cambios de las políticas.
d) Cumplimiento de los acuerdos por mandato jurisdiccional de los organismos de salud.
e) Mejoras recomendadas por profesionales de la salud y de la información, relacionadas a la protección de la información personal de salud.

7. Compromiso de la Subdirección.

La Subdirección de Tecnologías de Información, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos, se compromete a:

a) Promover en la Dependencia, las funciones y responsabilidades en el ámbito de seguridad de la información.
b) Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
c) Impulsar la divulgación y la concientización de la Política de Seguridad de la Información entre los servidores públicos, proveedores, terceros, entre otros.
d) Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
e) Considerar los riesgos de seguridad de la información en la toma de decisiones.
f) Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

La Secretaría de Salud y sus Órganos Descentralizados consideran que las funciones de Seguridad de la información deberán quedar integradas en todos los niveles jerárquicos de su personal.
Puesto que la seguridad de la información incumbe a todos los servidores públicos relacionados con la Secretaría de Salud y sus Órganos Descentralizados, esta política deberá ser conocida, comprendida y asumida por todos ellos, correspondientemente.

8. Principios.

Además, la Secretaría de Salud y sus Órganos Descentralizados establecen los siguientes principios básicos, como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

a) **Alcance estratégico:** La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de la Secretaría de Salud y sus Órganos Descentralizados, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

b) **Seguridad integral:** La seguridad de la información se entenderá como, un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

c) **Gestión de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

d) **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos, a la criticidad, valor de la información y de los servicios afectados.

e) **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

9. Políticas de seguridad de la información.

Las siguientes políticas de seguridad de la información son para proteger la información de Secretaría de Salud y sus Órganos Descentralizados.

9.1. Confidencialidad de la información.

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con Secretaría de Salud y sus Órganos Descentralizados o con su operación, será considerada información confidencial, tal como el acceso, intercambio y tratamiento de dicha información.

Solo podrá haber tratamiento de datos personales, cuando se cuente con el consentimiento de su titular o, en su defecto, se actualicen las hipótesis previstas en la Ley de Protección de Datos Personales del Estado de Chihuahua

Para obtener más información sobre la seguridad de la información consultar la política ***STI-POL-003 Política de Intercambio de Información.***

9.2. Propiedad intelectual.

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de Secretaría de Salud y sus Órganos Descentralizados.
Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.
Secretaría de Salud y sus Órganos Descentralizados únicamente autorizarán el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

9.3. Seguridad de datos personales.

Toda información de datos personales y datos personales sensibles proporcionados a la Secretaría de Salud y sus Órganos Descentralizados están protegidos y es tratados como confidencial. Los datos personales se tratan con las finalidades establecidas por Secretaría de Salud y sus Órganos Descentralizados, siempre contando con el consentimiento del titular.

a) **Datos Personales:** Cualquier información que se manifieste en forma numérica, alfabética, alfanumérica, grafica, fotográfica, acústica, o en cualquier otro formato, concerniente a una persona física identificada o identificable.
   Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

b) **Datos personales sensibles:** Aquellos que se refieran a la espera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este.

De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; estado de salud pasado, presente o futuro; información genérica o biométrica; creencias religiosas, filosóficas y morales; opiniones políticas y preferencia sexual.

Solo se tratarán los datos personales que resulten adecuados, relevantes y estrictamente necesarios. Toda información está protegida por la ***Ley de Protección de Datos Personales del Estado de Chihuahua*** así como los ***Lineamientos de la Ley de Protección de Datos Personales del Estado de Chihuahua.***

9.4. Intercambio de información.

Cualquier tipo de intercambio de información que se produzca entre Secretaría de Salud, sus Órganos Descentralizados y los proveedores de servicios, se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.
En relación con el intercambio de información se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transmisión o recepción de información sensible, salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con la dependencia.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.
- Todas las actividades que puedan dañar la imagen y reputación de Secretaría de Salud y sus Órganos Descentralizados están prohibidas en Internet y en cualquier otro lugar.

9.5. Uso apropiado de los recursos.

Los recursos de la Secretaría de Salud y sus Órganos Descentralizados, a los que se tengan acceso serán utilizados exclusivamente para cumplir con las obligaciones y propósitos de la provisión del servicio.
Bajo ningún concepto podrán ser utilizados para actividades no relacionadas con el propósito del servicio o para la comisión de actividades que pudieran ser consideradas ilícitas, como daños contra la propiedad intelectual de terceros, incumplimientos de la normativa de protección de datos etc.

Con el fin de velar por el correcto uso de los mencionados recursos, Secretaría de Salud y sus Órganos Descentralizados, podrán implementar los mecanismos de control necesarios, de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.
En caso de apreciar que algún usuario, utiliza incorrectamente los recursos o información de Secretaría de Salud o de alguno de sus Órganos Descentralizados, se reportará a la Subdirección de Tecnologías de Información para que realice las acciones oportunas.
La Secretaría de Salud y sus Órganos Descentralizados se reservan el derecho de ejercer las acciones que legalmente le amparen para la protección de sus derechos.
Cualquier fichero introducido en la red de Secretaría de Salud y sus Órganos Descentralizados o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal, y control de virus y programa maligno.

9.6. Responsabilidades de usuario.

Los usuarios que tengan acceso a la información, sistemas de información o recursos de la Secretaría de Salud y sus Órganos Descentralizados deberán respetar los siguientes principios básicos dentro de su actividad:

- Cumplir con los puntos descritos en ***FR-POL-001 Responsiva de claves de acceso asignadas para uso de los sistemas informáticos,*** debidamente firmada por el usuario.
- Cada persona con acceso a información de Secretaría de Salud o de alguino de sus Órganos Desentralizados, es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier persona con acceso a información de Secretaría de Salud y sus Órganos Descentralizados, deberán velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier persona con acceso a información deberá respetar las normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera

del mismo (Almacenamiento bajo llave, bloqueo de equipos desatendidos, protección de los puntos de recepción y envío de información, destrucción segura, etc.)

- Las personas con acceso a sistemas de información de Secretaría de Salud y sus Órganos Descentralizados, por ningún motivo deberán, realizar pruebas para detectar y/o explotar una supuesta debilidad o incidencia de seguridad, sin previa autorización por escrito.
- Ninguna persona con acceso a sistemas de información de Secretaría de Salud o alguno de sus Órganos Descentralizados, intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, sin autorización expresa por escrito. Se prohíbe la captura de tráfico de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.

9.7. Requisitos de seguridad para los dispositivos.

Todos los dispositivos con acceso a información de Secretaría de Salud y sus Órganos Descentralizados, independientemente de la propiedad de estos, deberán cumplir con las políticas de seguridad establecidas aquí mismo, en especial se tendrán en cuenta las siguientes consideraciones:

- El acceso a los sistemas deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador personal y una contraseña asociada.
- Los dispositivos deberán permanecer actualizados con la última versión disponible de parches de seguridad para el software y sistema operativo instalado.
- Los dispositivos deberán contar con un sistema de protección anti-malware instalado, activo y actualizado a su última versión disponible, tanto del motor como del fichero de firmas (actual mente en la Secretaría de Salud y sus Órganos Descentralizados se maneja la solucion FORTI-EDR).
- Deberá activarse el bloqueo de pantalla para que este salte a los 10 minutos de inactividad. El desbloqueo deberá conllevar el uso de contraseñas, patrones de desbloqueo o mecanismos equivalentes, que garanticen que el dispositivo no podrá ser utilizado por un usuario no autorizado.
- Los dispositivos no dispondrán de ninguna herramienta o ficheros que pueda interferir con el software corporativo. Este punto incluye, aquellos que traten de descubrir información distinta de la del propio usuario o realizar accesos no autorizados, como por ejemplo sniffers, herramientas de escaneo de redes, descubrimiento de contraseñas, etc.

9.8. Comunicación de incidentes de seguridad.

Los usuarios se comprometen a comunicar de manera inmediata a la Subdirección de Tecnologías de Información a través del responsable del servicio cualquier incidente, debilidad o amenaza

(observada o sospechada) que detecte en los sistemas de información de Secretaría de Salud o de sus Órganos Descentralizados, que haya podido afectar a información propiedad de los mismos.

Tratándose de datos personales y datos personales sensibles a su vez deberá comunicarse al Comité de Transparencia de Secretaría de Salud o de sus Órganos descentralizados para notificación al organismo garante en caso de afectación en los derechos morales o patrimoniales de confidencialidad.

9.9. Seguridad en desarrollo.

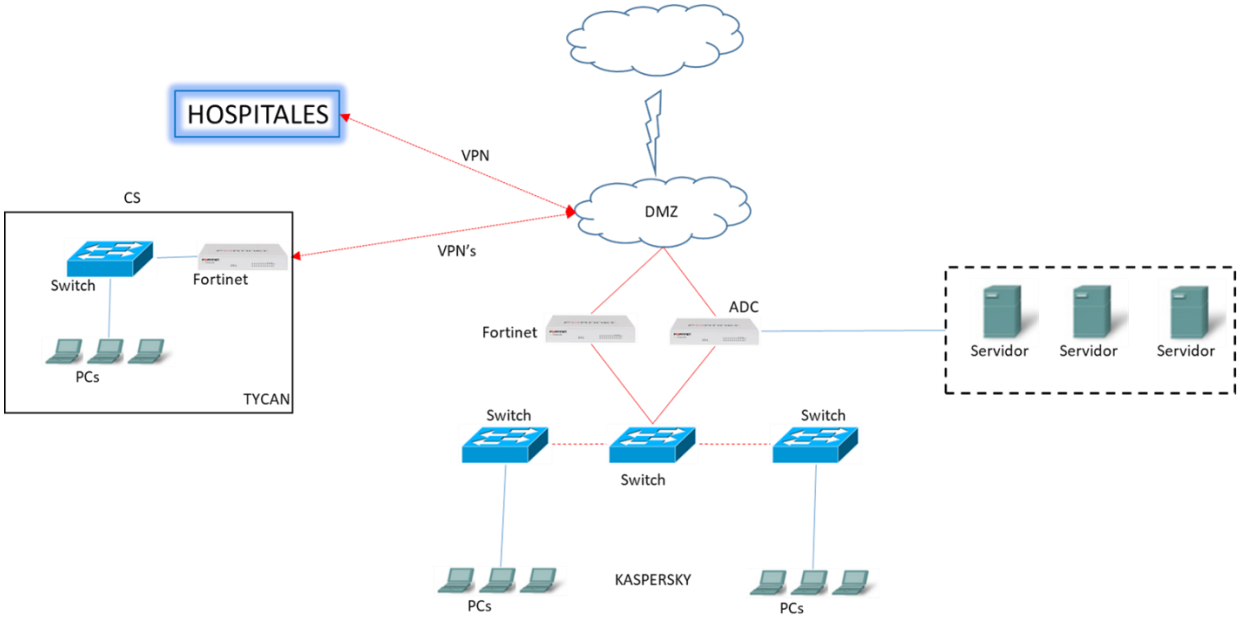
Obligados: Todos los usuarios que realicen trabajos de desarrollo y/o pruebas de aplicaciones para Secretaría de Salud y sus Órganos Descentralizados.

- Los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción.
- Todos los accesos a los sistemas de información que alberguen o procesen información deberán estar protegidos, al menos, por un “Firewall”, que limite la capacidad de conexión a ellos.
- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por personal de la Secretaría de y sus Órganos Descentralizados.
- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
- Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
- En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

- Solo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

9.10. Seguridad de la red.

- Todas las redes estan adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados, ni conexiones cuyos riesgos no estén apropiadamente gestionados por él, estableciéndose los oportunos sistemas de monitorización y auditoría de seguridad necesarios para garantizar la seguridad de las conexiones.
- La infraestructura de la red esta protegida tanto de internet hacia adentro como de adentro hacía internet.
- Desde internet hacia adentro exite una DMZ protegiendo los paquetes que entran a la red de la Secretaría de Salud y sus Órganos Descentralizados, continuando el flujo por Fortinets especializados con configuraciones especificas a el proposito de protección de información.
- Dentro de la red local, cada usuario cuenta con un antivirus conectado a un servicio de proveedor especifico en seguridad.
- Para las conexiones a las Jurisdicciones remotas se emplean VPN’s seguidas por Fortinets, con apoyo para la administración por un proveedor.
- Las redes que permitan el acceso a la infraestructura Secretaría de Salud y sus Órganos Descentralizados deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:
    - Deberán ser comunicadas y autorizadas por medio de solicitudes de usuarios para VPN’S a la Subdirección de Tecnologías de Información.
    - El acceso de usuarios remotos a la red de Secretaría de Salud y sus Órganos Descentralizados estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.
    - Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales líneas dedicadas.
    - En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas


HOSPITALES
VPN
VPN's
DMZ
CS
Switch
Fortinet
PCs
TYCAN
Fortinet
ADC
Servidor
Servidor
Servidor
Switch
Switch
Switch
PCs
KASPERSKY
PCs