Equipo y Tecnología para el cuidado de la vida

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Tecnología de la Información

Política de Seguridad de la Información

Código: MSG-01

Elaboró:	Revisó:	Autorizó:
Erick Martínez Coordinador de Tecnología	Pedro Colina Macedo Coordinación del Sistema de Gestión de la Calidad	Rodolfo Davis Contreras Dirección de Operaciones

Fecha de Autorización: 3 de febrero de 2023
No. de revisión: 14

1. POLÍTICA DE SEGURIDAD

Equiver comprometido con la seguridad de la información redacta este documento con la finalidad de establecer una política de seguridad que minimice los posibles riesgos de seguridad de la información en su operación, planteando los detalles que deberá tomar en cuenta, así como los controles que se aplicarán.

Las políticas y lineamientos aplican para todas las áreas, incluyendo el personal bajo contrato por tiempo determinado, los proveedores y todos los sistemas informáticos y de comunicaciones utilizados por el personal y la empresa. Estos sistemas incluyen las redes de área local, las computadoras personales (PC) y demás sistemas administrativos, los centros de procesamiento locales de cómputo, de telecomunicaciones y de conmutación, los proveedores de servicios de Internet (ISP) y otros proveedores externos de servicios de información.

1.1 Política de seguridad de la información

1.1.1 Documento de política de seguridad de la información

El presente documento conforma en su totalidad el documento de política de seguridad de la información de Equiver.

A lo largo del presente documento se establecen las necesidades, objetivos, alcance, requisitos, estándares y disposiciones que observará Equiver como parte de la implementación del sistema de gestión de seguridad de la información.

1.1.2 Revisión de la política de seguridad de la información

La política de seguridad de la información será revisada cada 12 meses o antes si existiera algún cambio de las responsabilidades de la seguridad de la información o significativo en los estándares internacionales, y si fuera necesario, se publicará nuevamente.

Entre las principales causales de revisión de la presente política de seguridad de la información se encuentran:

- Nuevos riesgos identificados
- Actualización de infraestructura tecnológica
- Mejores prácticas internacionales y recomendaciones
- Actualizaciones de normatividad, legislación y regulaciones aplicables

2. Aspectos organizativos de seguridad de la información

2.1 Organización interna

2.1.1 Compromiso de la dirección con la seguridad de la información

La Dirección General apoyará activamente la cultura sobre seguridad de la información a través de una directrices claras, asignación explícita y reconocimiento de las responsabilidades según corresponda.

La Dirección general designará a una persona o grupo encargado de conocer y aplicar la política de seguridad descrita en el presente documento.

Con el fin de hacerse cargo del monitoreo y seguimiento a los detalles de seguridad que se puedan dar en la

operación, el encargado de seguridad debe tener conocimiento de Tecnologías de la Información (TI) que le permita realizar su labor.

Así mismo, la Dirección conformará un grupo seguridad de la información (GSI), el cual se encargará de la coordinación y seguimiento a la implementación de los controles de seguridad descritos en la presente política de seguridad. De acuerdo con la estructura orgánica de Equiver, el GSI estará conformado por:

Responsable de TI	CARGO: Analista de Tecnología FUNCIONES: ● Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del SGSI, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo. ● Asegurar la disponibilidad de los recursos necesarios de telefonía y equipo de cómputo del personal en general para el cumplimiento de sus programas de trabajo. ● Cumplir con los programas de mantenimiento establecidos, a fin de garantizar el buen funcionamiento de los recursos asignados. ● Primer nivel de respuesta ante incidentes. ● Soporte a usuarios. ● Alta, baja y modificación de accesos a sistemas y aplicaciones. ● Gestión de parches de seguridad informática. ● Seguridad de la Información
Responsable de calidad	CARGO: Coordinación del S.G.C. FUNCIONES: ● Elaboración y seguimiento de la documentación de los procesos. ● Apoya en el diseño y desarrollo de documentos necesarios en términos de requerimientos del Sistema de Gestión. ● Identificar oportunidades de mejora de los procesos. ● Incorporar conceptos de calidad y mejora continua a la operación de la empresa. ● Desarrollo y atención de auditorías. ● Cumplimiento de las políticas y normas establecidas en materia de seguridad. ● Administrar documentación del tema de Seguridad e Higiene de los Centros de trabajo para cumplir los lineamientos que marca Protección Civil. ● Planificar, organiza los programas de mantenimiento del sistema de alarma y detección de humos e incendio, equipo de extinción portátil. ● Coordinar reuniones de seguridad de la información.
Responsable de operaciones	CARGO: Coordinador de Tecnología FUNCIONES: ● Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI ● Planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el SGSI. ● Planear las actividades necesarias para una adecuada administración y sostenibilidad del SGSI

	• Supervisar, coordinar y controlar las operaciones y políticas de seguridad vigentes. • Identificación, evaluación y optimización de recursos operativos para la seguridad de la información. • Trabajar de manera integrada con el grupo o áreas asignadas en materia de seguridad de la información. • Velar por el mantenimiento de la documentación del SGSI, su custodia y protección. • Gestionar y coordinar los recursos necesarios relacionados con el desarrollo e implementación de sistemas de la información. • Definición de la estrategia de seguridad informática. • Detección de necesidades y vulnerabilidades de seguridad. • Implementación, configuración y operación de los controles de seguridad informática. • Monitoreo de indicadores de controles de seguridad. • Seguridad de la Información

Entre otras funciones, el GSI llevará a cabo reuniones de trabajo relacionadas con la seguridad de la información. El objetivo del grupo será encontrar oportunidades de mejora y la necesidad de aportar cambios mediante revisiones que deben estar documentadas y registradas, así como coordinarse con las diferentes direcciones y áreas para la toma de decisiones y acciones relacionada con la seguridad de la información.

Finalmente, la Dirección de Equiver declara que el alcance de seguridad de la información para la empresa está delimitado por la información en salud que se maneja dentro de la misma y es por ello que los controles de seguridad que se apliquen derivado de la presente política de seguridad estarán enfocados en aquellos activos relacionados con la información en salud.

2.1.2 Coordinación de la seguridad de la información

El GSI identificará a los responsables de cada una de las diferentes áreas que conforman la estructura orgánica de Equiver, a fin de identificar y asignar las correspondientes funciones referentes al manejo seguro de la información, así como el rol que desempeñarán dentro de la política de seguridad de la información.

Con el presente control de seguridad, el GSI comunicará al personal de Equiver la relevancia de alcanzar los objetivos de seguridad de la información y su participación en la misma, a fin de que sea acatada y se conozcan las consecuencias de su omisión.

2.1.3 Asignación de responsabilidades relativas a la seguridad de la información

El GSI, con base a un previo análisis, informará explícita y formalmente a los encargados de las áreas principales que conforman la estructura orgánica de Equiver las funciones de seguridad que deberán observar en sus labores. Dicho personal designado firmará de conocimiento.

2.1.4 Proceso de autorización de recursos para el tratamiento de la información

Para tener un control de todos los recursos que se deberán administrar como parte del SGSI, cada nuevo recurso de información deberá darse de alta en el registro de activos relacionados con el tratamiento de la información y se deberá formalizar el apego de dicho recurso a la política de seguridad a través del formato que para este fin se haya establecido, mismo que contendrá:

- Tipo de recurso
- Nombre
- Descripción
- Información que manejará o con la que interactúa
- Fecha de alta

2.1.5 Acuerdos de confidencialidad

Todo el personal que labora en Equiver firmará una Carta de Confidencialidad mediante el cual quedará formalmente notificado de su responsabilidad respecto del apego a la política de seguridad de la información y las sanciones correspondientes en caso de su incumplimiento u omisión. Esto aplicará tanto para el personal interno como externo en caso de no contar con dicho acuerdo en el contrato de servicios.

2.1.6 Contacto con las autoridades

Debido a la naturaleza del entorno en donde Equiver lleva a cabo sus operaciones tanto internamente como con sus clientes, se considera el siguiente directorio de autoridades que serán contactadas en caso de surgir alguna situación que comprometa la seguridad de la organización o quienes la conforman.

Autoridad	Domicilio / ubicación	Contacto	Llamar en caso de:
Emergencias	Todo el país	911	Cualquier emergencia de seguridad.
Cruz Roja Mexicana	Anillo Periférico (Blvd. Adolfo Ruiz Cortines) 7666, Hueso Periférico, 14338 Ciudad de México, CDMX	065 y 53-95-11-11	Riesgos contra la salud.
Protección civil	Viaducto Tlalpan S/N, Antiguo Ejido Viejo de Santa Úrsula Coapa, 04980 Coyoacán, CDMX	56-83-22-22	Sismo, incendio, inundación
Policía	Anillo Periférico 3648, Jardines del Pedregal, 10400 Ciudad de México, CDMX	066 y 52-42-51-00	Denuncias
Bomberos	Canal Nacional 1130, Coyoacán, San Francisco Culhuacán, 04480 Ciudad de México, CDMX	068 y 57-68-37-00	Incendio, inundación.
Ciberseguridad	Liverpool No. 136, Col. Juárez, C.P. 06600, Tel. 5242 5100	52089898	Ataques cibernéticos de seguridad.

2.1.7 Contacto con grupos de especial interés

El GSI estará en contacto con grupos de profesionales de la seguridad de la información, con la finalidad de mantenerse actualizados con métodos o técnicas de protección de información más efectivas. Estos grupos serán consultados de manera periódica.

Descripción	Organización	Contacto	Frecuencia
Comunicados, noticias referentes a la seguridad informática o información	Bitdefender	https://www.bitdefender.com/blog/labs/	Mensual
Noticias, opiniones y análisis de la comunidad de seguridad de ESET	ESET	https://www.welivesecurity.com/la-es/	Mensual
Noticias, tips, y recomendaciones sobre seguridad de la información	Microsoft	https://www.microsoft.com/security/blog/	Mensual
Artículos referentes a la seguridad de la información.	Organización Internacional de Normalización	https://www.iso.org	Mensual

2.1.8 Revisión independiente de la seguridad de la información

A petición de la dirección, se realizarán evaluaciones del sistema de gestión de seguridad de la información mismas que se llevarán a cabo por personal externo.

2.2 Terceros

2.2.1 Identificación de los riesgos derivados del acceso de terceros

El GSI identificará los riesgos que impliquen las personas ajenas a la empresa Equiver, se documentará en la Matriz de Riegos, e indicarán los controles de seguridad a implantar previo a otorgar acceso a un tercero a la información en salud manejada por Equiver. El análisis se puede verse en el documento “ANÁLISIS DE RIESGOS”.

2.2.2 Tratamiento de la seguridad en la relación con los clientes

Como parte del tratamiento de la información, Equiver ha establecido el siguiente decálogo de seguridad, al cual se deberá apegar todo aquel usuario al que se le brinde acceso a la información en salud dentro de Equiver:

I. Las contraseñas son personales e intransferibles.
II. No se permiten los accesos indebidos o a través de canales no autorizados.
III. Queda estrictamente prohibido el uso de la información para fines distintos a los que originalmente se definieron.
IV. Toda la información deberá ser manejada bajo los principios de confidencialidad y no difusión de la información.
V. Todos los riesgos de seguridad de la información deberán ser notificados al GSI.
VI. Cualquier acto ilícito relacionado con el manejo de seguridad de la información deberá ser notificado al GSI.
VII. Queda prohibida la extracción no autorizada de información de cualquiera de los activos de información identificados.
VIII. Queda prohibido llevar a cabo ataques que atenten contra la integridad, disponibilidad y accesibilidad de la información.
IX. El intercambio de información se deberá llevar a cabo conforme a los lineamientos que para este fin se han establecido en la presente política de seguridad de la información.
X. Cualquier medida adicional de seguridad que permita salvaguardar la integridad, disponibilidad y

accesibilidad de la información deberá ser aplicada con independencia de si ésta se encuentra considerada en la política de seguridad.

2.2.3 Tratamiento de la seguridad en contrato con terceros

Para el caso específico de personal externo a Equiver, deberán firmar un acuerdo de confidencialidad y no divulgación donde se les informe de la existencia de una política de seguridad, así como las sanciones a las que estén sujetos por incumplimiento de estas.

Dicho compromiso será formalizado a través del respectivo contrato de servicios, la herramienta o el documento que para este fin se defina.

3. Gestión de activos

3.1 Responsabilidad sobre los activos de Salud

3.1.1 Inventario de activos

Equiver generará y mantendrá una relación de los activos de información. Para cada activo, en dicha relación se tendrán por lo menos en caso de aplicar los siguientes datos:

- Identificador del activo
- Tipo de activo (lógico/físico)
- Nombre del activo
- Descripción del activo
- Prioridad del activo (alta/media/baja)
- Uso adecuado del activo
- Propietario o responsable del activo

En el anexo “Inventario de Activos” se encuentra el listado completo que contiene el detalle de activos.

3.1.2 Propiedad de los activos

Equiver a través del inventario de activos, descrito en el numeral 3.1.1 de la presente política de seguridad de la información, identificará al propietario de cada uno de los activos de información que forman parte del alcance de la presente política de seguridad de la información.

Cada propietario, de acuerdo con la relación de activos de información, deberá mantener el listado de dicho inventario actualizado. Por su parte, el GSI podrá mantener informado al propietario del activo sobre su responsabilidad asociada con una cláusula de compromiso.

3.1.3 Uso aceptable de los activos de Salud

Equiver a través del inventario de activos descrito en el numeral 3.1.1 de la presente política de seguridad de la información, establecerá el uso que se deberá dar para aquellos activos de información y se añade la cláusula de compromiso.

3.2 Clasificación de la información de salud

3.2.1 Lineamientos de clasificación

Equiver en su inventario de activos, descrita en el numeral 3.1.1 de la presente Política de Seguridad de la Información, clasifica los activos de información de salud de acuerdo con su prioridad (alta, media o baja), tomando en cuenta su sensibilidad, criticidad, requisitos legales y aquellos que se consideren pertinentes.

3.2.2 Etiquetado y manipulado de la información

Todo aquel activo de información que se encuentre dentro del alcance de la presente política de seguridad contará con una leyenda visible que permita identificar al portador o usuario de esta, que dicha información se encuentra sujeta a políticas de seguridad de la información. Dicha leyenda se habilitará principalmente en los sistemas de información en salud y medios impresos relacionados.

4. Seguridad en Recursos Humanos

4.1 Antes del empleo

4.1.1 Funciones y responsabilidades

El personal interno deberá conocer para dar cumplimiento como parte de sus actividades dentro y fuera de la empresa maneje, administre o interactúe con información en salud tendrá funciones y responsabilidades, mismas que serán de su conocimiento a través del documento Descripción del Puesto y deberá firmar de conocimiento.

4.1.2 Investigación de antecedentes

Las áreas que dentro de Equiver se encarguen de llevar a cabo contratación de personal interno, realizarán las diligencias correspondientes para conocer de cada uno de ellos, cuando la Dirección así lo solicite o cuando mejor se determine, los antecedentes personales o empresariales, tomando en consideración los siguientes datos y/o documentos:

- Verificar la identidad del candidato/empresa.
- Contar con Curriculum Vitae, dentro del cual se pueda validar mediante referencias la información plasmada.
- Domicilio
- Verificar referencias de empleos o proyectos anteriores
- Los terceros deben de contar con el entrenamiento adecuado sobre las políticas y procedimientos de seguridad de la organización.

El personal que se encargue de llevar a cabo contratación de personal interno, deberá mantener los registros de dicha investigación.

4.1.3 Términos y condiciones de empleo

El personal interno de Equiver que procesa información personal de salud tendrán conocimiento de las condiciones de seguridad, las sanciones, cláusulas y responsabilidades relacionadas con la seguridad de la información en salud. Para garantizar, podrán firmar y aceptar el acuerdo de confidencialidad y no divulgación donde

se les informe de la existencia de una política de seguridad, así como las sanciones a las que estén sujetos por incumplimiento u omisión de estas.

4.2 Durante el empleo

4.2.1 Responsabilidades de la Dirección

La Dirección de Equiver apoyará activamente la política de seguridad de la información a través de una dirección clara, asignación explícita y reconocimiento de las responsabilidades según corresponda, así como las sanciones pertinentes para hacer cumplir la política vigente.

Dicho apoyo se realizará mediante la comunicación al personal de la relevancia de alcanzar los objetivos de seguridad de la información, acatar la política creada, la necesidad de una mejora continua y la necesidad de aportar cambios mediante revisiones documentadas.

4.2.2 Concienciación, formación y capacitación en seguridad de la información

El GSI proporcionará a los empleados de la organización, los contratistas y terceros responsables de procesar información personal de salud, programas de concientización, educación y capacitación en función de las necesidades de la empresa, para que éstos a su vez lo transmitan hacia los usuarios de los activos de información.

El personal recibirá capacitación, de manera que se mantenga actualizado y comprometido con la seguridad de la información.

Para afianzar la cultura de seguridad de la información, se hará la difusión correspondiente mediante cualquiera de los siguientes medios:

- Capacitaciones en materia de seguridad de la información
- Carteles o trípticos en materia de seguridad

4.2.3 Proceso disciplinario

Las políticas y lineamientos de Seguridad de la Información deben cumplirse en todo momento. Cualquier incumplimiento será tratado de acuerdo con los procedimientos disciplinarios dispuestos por la Equiver.

Ante cualquier situación generada, en la cual se ponga en riesgo la seguridad de la información, o dicho riesgo se haya materializado, afectando activos de información, a través del GSI se determinará las acciones correctivas correspondientes, incluyendo las sanciones aplicables, dentro de las cuales se tendrán:

- Amonestación privada. Llamada de atención personal y en privado al causante. Se tomará como un primer antecedente.
- Amonestación pública. Se hará de conocimiento del personal que así considere pertinente la Dirección, sobre la falta que llevó a cabo el causante. Así mismo.
- Suspensión temporal. En caso de que la afectación haya sido considerada grave, la Dirección podrá tomar la decisión de suspender temporalmente las actividades laborales, servicio o contrato con la parte causante, misma que perderá cualquier derecho o recurso de defensa.
- Suspensión definitiva. En caso de que la afectación haya sido considerada grave o muy grave, la Dirección podrá tomar la decisión de suspender definitivamente las actividades laborales, servicio o contrato con la parte causante, misma que perderá cualquier derecho o recurso de defensa.

4.3 Cese del empleo o cambio de puesto de trabajo

4.3.1 Responsabilidad del cese o cambio

Al momento de notificar la terminación del contrato de un empleado, contratista o tercero por cualquier motivo y en cualquier circunstancia, el GSI debe considerar y cuando corresponda garantizar que:

a) Se eliminan los derechos de acceso a los sistemas, cuentas de correo electrónico, acceso a Internet, aplicativos y demás activos de información a los que pueda existir un uso o acceso no autorizado.

b) La correspondiente área contratante, informará al SGI sobre cualquier terminación de contrato de personal o externos.

c) En caso de representar un riesgo significativo para los activos de información de Equiver, el sujeto en cuestión podrá ser llevado fuera de las instalaciones y se le deniegue el acceso a las mismas en el futuro.

d) Se deben de retirar los permisos de acceso del empleado o terceros contratados como pueden ser:

- Accesos físicos a la institución
- Servicios de red
- Software, los equipos, manuales y demás documentación de informática;

Cuando se le permita al empleado o tercero continuar con sus funciones, se mantendrá vigilado para detectar cualquier actividad o comportamiento inusual.

e) Los empleados y terceros contratados deben de regresar los activos propiedad de la organización utilizados durante su trabajo en el tiempo que duró su contrato.

Los activos utilizados son:

- Software
- Hardware
- Equipo de Oficina y/o documentos corporativos
- Información en medios electrónicos y credenciales de acceso.

4.3.2 Devolución de activos

Para garantizar que todos los activos sean devueltos al momento de notificar la terminación del contrato de un empleado, contratista o tercero se deberá:

- Cotejar en el Inventario de Activos a los cuales se le dio acceso a la persona, mismo que firmó de conocimiento, validando que todos los accesos, posesión o disponibilidad, queden inhabilitados por completo.
- Llenar el formato de confirmación de baja y devolución de activos.

El formato de confirmación de baja podrá incluir:

- Todos los activos que se están entregando y el estatus de la entrega.
- En caso de que alguno deba ser cambiado o eliminado deberá incluir si ya fue realizada la acción.
- Firma del responsable que recibe, constatando que todas las acciones de cese se llevaron a cabo.

4.3.3 Retirada de los derechos de acceso

Al momento de notificar la terminación del contrato de un empleado, contratista o tercero por cualquier motivo, se notificará al GSI para la suspensión de todos los derechos de acceso a cualquier activo de información al que haya tenido acceso.

5. Seguridad Física y del entorno

5.1.1 Perímetro de seguridad física

La Dirección velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro principalmente de aquellas instalaciones bajo las cuales se resguardan activos de información.

Así mismo, mediante controles de seguridad buscará mitigar el impacto de riesgos tales como: las amenazas físicas externas e internas y las condiciones medioambientales.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

5.1.2 Controles físicos de entrada

Debe protegerse la seguridad física de las instalaciones y del personal de Equiver:

- Se proporcionará una identificación adecuada para cada empleado de la empresa, la cual debe ser portada en todo momento dentro de las instalaciones.
- Solamente el personal autorizado pueda acceder a las instalaciones.
- Los equipos y dispositivos de almacenamiento, procesamiento y transmisión de información estarán dentro de los perímetros de las áreas de seguridad, mismas que serán resguardadas y a las cuales solamente se le permitirá el acceso al personal autorizado.
- Siempre que sea posible, se utilizará sistemas automatizados de control de acceso físico.
- El acceso a las áreas seguras debe ocurrir solamente cuando exista la justificación pertinente.
- De ser posible, se implementarán sistemas de grabación o circuito cerrado.
- Las instalaciones de Equiver contarán con personal de recepción encargado de los accesos.

5.1.3 Seguridad de oficinas, despachos e instalaciones

El GSI implementará las medidas de seguridad en las áreas internas de las instalaciones, tales como:

- Candados de seguridad.
- Llaves únicas para cajoneras.
- Llaves únicas para oficinas, despachos y salas de juntas.

Así como aquellos que se incorporen a través del tiempo de acuerdo con las necesidades detectadas.

5.1.4 Protección contra las amenazas externas y de origen ambiental

Los factores externos tales como temperatura, la humedad y la ventilación dentro de las instalaciones que albergan equipos de cómputo, comunicaciones y medios de almacenamiento de información se mantendrán bajo condiciones ambientales favorables, a fin de evitar el daño a dichos equipos.

Así mismo, las instalaciones tendrán protección contra daños de origen ambiental o daños naturales, tales como:

- Detectores de humo.
- Extintores.
- Rutas de evacuación.

Se podrán incorporar nuevos elementos de protección contra daños de origen ambiental según se identifique.

5.1.5 Trabajo en áreas seguras

Las áreas de trabajo deben ser seguras para que el personal pueda realizar su labor, y en aquellas áreas donde tengan restricciones particulares se debe notificar al personal cuales son las medidas de seguridad adecuadas, tales como: precaución con altos voltajes, precaución con líquidos o alimentos, precaución con artefactos magnéticos o de interferencia.

Todas estas restricciones deben estar señalizadas en forma de avisos o carteles de seguridad en el entorno de trabajo.

También deben estar correctamente señalizadas, las rutas de evacuación, así como extintores y salidas de emergencia.

5.1.6 Áreas de acceso público y de carga y descarga

Este control no aplica.

5.2 Seguridad de los equipos

5.2.1 Emplazamiento y protección de equipos

El equipo de cómputo y de procesamiento de información estará debidamente resguardado o provisto con mecanismo de protección para evitar que pueda ser extraído por personal no autorizado.

De igual forma estará protegido contra accesos no autorizados al equipo o extracción de información por personal ajeno o no autorizado. Para ello se tomarán en cuenta los siguientes lineamientos:

a) Los equipos estarán asegurados físicamente al inmueble, ya sea empotrados o asidos a una estructura para evitar su extracción.
b) Si los equipos son móviles como laptops contarán con un candado de seguridad mientras estén en las instalaciones o lugares de trabajo.
c) Los equipos tendrán contraseñas de acceso.
d) El equipo tendrá una directiva de seguridad de auto-bloqueo de sesión por inactividad.

5.2.2 Instalaciones de suministro

Las instalaciones de Equiver cuentan con un sistema de suministro eléctrico confiable para evitar fallos en los equipos de cómputo y de procesamiento de la información.

Las instalaciones cuentan con:

- Cableado estructurado.
- Regulación eléctrica adecuada.

5.2.3 Seguridad del cableado

Las instalaciones de Equiver cuentan con controles de acceso restringido al cableado eléctrico y de red, con el fin de evitar interrupciones o ataques de algún tipo a esta infraestructura.

5.2.4 Mantenimiento de los equipos

Los equipos se mantendrán en buen estado para su correcto funcionamiento, por lo tanto, el área de TI brindará el soporte correspondiente a los equipos. Para cada mantenimiento ya sea correctivo o preventivo, se llenará un formato de mantenimiento, el cual registrará los siguientes datos:

- Identificador del equipo
- Fecha del mantenimiento aplicado
- Tipo de mantenimiento.
- Observaciones
- Firma del responsable del mantenimiento

5.2.5 Seguridad de los equipos fuera de las instalaciones

Todo el equipo de Equiver que sea sacado de las instalaciones de esta, incluyendo computadoras portátiles, unidades de almacenamiento, otros dispositivos electrónicos contarán con protección contra robo y pérdidas.

La provisión y utilización de equipos de la empresa fuera de las instalaciones será autorizada por la Dirección o GSI, tomando en cuenta los riesgos involucrados. El personal a cargo del equipo fuera de las instalaciones es responsable de:

a) Proteger la confidencialidad de la información.
b) La seguridad e integridad física de ese equipo.
c) Garantizar que el equipo sea utilizado sólo para los propósitos autorizados y por personal autorizado.
d) Utilizar los controles de seguridad provistos con el equipo, tales como cerraduras físicas y sistemas de cifrado de archivos en caso de que el equipo contenga información confidencial o de salud.
e) Almacenar de manera segura las unidades magnéticas extraíbles cuando no se estén utilizando.
f) Desconectar el equipo de las redes de telecomunicaciones cuando no se esté utilizando.

Para autorizar el uso del equipo fuera de la empresa se debe llenar el formato de autorización correspondiente e ir firmado por la dirección.

5.2.6 Reutilización o retirada segura de equipos

Todo el equipo de la empresa que sea retirado por reemplazo o que su vida útil haya terminado será sometido a un procedimiento de borrado por completo, es decir:

- Se identificarán los medios de almacenamiento de la información y estos deben ser borrados con software de borrado seguro que sobrescriba la información.
- Si el medio de almacenamiento no es accesible por software será destruido o desarmado físicamente.
- una vez concluido el proceso de borrado se llenará el formato de retirada segura de equipos el cual deberá tener los siguientes datos:
    - Destino del equipo
    - Información que almacenaba
    - Motivo del retiro
    - Observaciones
    - Firma del encargado de eliminar la información
    - Aprobación de la dirección

5.2.7 Retirada de materiales propiedad de la organización

Todo activo que sea retirado o reubicado ya sea dentro de la empresa o fuera de ella, será autorizado por

la dirección, llamándose un documento de autorización con los siguientes datos:

- Destino del activo
- Información que almacena
- Motivo del retiro o movimiento
- Observaciones
- Firma del encargado de eliminar la información
- Aprobación de la dirección

6. Seguridad Física y del entorno

6.1. Responsabilidades y procedimientos de operación

6.1.1. Documentación de los procedimientos de operación

Los procedimientos de la operación y el manejo de la información en salud de Equiver a través del sistema SIDECAM se establecen en el documento denominado “Manual de Usuario”. Los usuarios y personal que interactúe con dicha información deberán apegarse al uso y recomendaciones establecidas en dicho documento.

6.1.2. Gestión de cambios

Los cambios y actualizaciones de los sistemas de manejo de la información en salud serán autorizados por algún miembro del GSI antes de ser aplicados en ambientes de producción. Dichas modificaciones serán formalizadas de acuerdo con el Procedimiento Gestión de Cambios.

6.1.3. Segregación de tareas

Para el sistema SIDECAM existirá una matriz de roles y perfiles que acoten las funciones del sistema de acuerdo con los usuarios: administrador de pacientes, unidad médica, laboratorio y administrador.

6.1.4. Separación de los recursos de desarrollo, prueba y operación

Se contará con un ambiente de pruebas y desarrollo, separados física y virtualmente del ambiente productivo, todos ellos asociados al sistema SIDECAM.

6.2. Gestión de la provisión de servicios por terceros

6.2.1. Provisión de servicios

Los proveedores al servicio de Equiver formalizarán sus funciones a través de un contrato. Se establecerán sus actividades y alcances iniciales. Los requerimientos adicionales se registran de acuerdo con el procedimiento de Gestión de Cambios para evaluación, alcance y autorización.

6.2.2. Supervisión y revisión de los servicios prestados por terceros

Los servicios prestados por terceras partes serán monitoreados por el GSI de acuerdo con el procedimiento PTI-04 Procedimiento de Supervisión y Seguimiento de Proyecto.

6.2.3. Gestión del cambio en los servicios prestados por terceros

Toda actualización o cambio en los servicios prestados por terceros estará monitoreada y documentada para su aprobación por parte del GSI, de acuerdo con en el procedimiento Gestión de Cambios.

6.3. Gestión de la provisión de servicios por terceros

6.3.1. Gestión de capacidades

El sistema SIDECAM será analizado periódicamente de acuerdo con lo que el GSI defina para precisar el rendimiento actual y estimar un rendimiento futuro, de tal forma que se garantice un funcionamiento óptimo en la operación.

6.3.2. Aceptación del sistema

Los cambios, modificaciones o actualizaciones de los sistemas de manejo de información deben ser evaluados en un ambiente de pruebas para ser aprobados.

Se deberá hacer la solicitud de acuerdo con el procedimiento de Gestión de Cambios.

Una vez que hayan sido probados los cambios, si las pruebas son satisfactorias deben ser aprobadas por algún integrante del Grupo de Seguridad de la Información y/o la Dirección, para su puesta en marcha.

6.4. Protección contra el código malicioso y descargable

6.4.1. Controles contra el código malicioso

Los equipos de cómputo de Equiver tendrán software que detecte, bloquee y elimine virus u otros códigos maliciosos, mismo que se mantendrá actualizado y con las licencias pertinentes para su buen funcionamiento. Adicionalmente los sistemas operativos de dichos equipos estarán actualizados.

Para SIDECAM, la infraestructura tendrá un balanceador con el acceso o bloqueo de puertos establecidos en el documento Controles contra el código malicioso, configurado un Firewall y adicional el acceso a la BD por medio del IP autorizadas.

6.4.2. Controles contra el código descargado en el cliente

Los equipos de cómputo de Equiver tendrán protección que detecte la descarga de archivos maliciosos o bloqueo de páginas de internet que puedan contener códigos que puedan afectar el funcionamiento y la integridad de la información, así como correo electrónico no deseado y potencialmente peligroso.

6.5. Copia de seguridad de información de salud

6.5.1. Copias de seguridad de la información en Salud

Toda la información de salud será respaldada periódicamente dependiendo de la criticidad de la información siguiendo lo indicado en el documento: Copias de Seguridad de la Información en Salud. Los respaldos de información serán sometidos a pruebas que confirmen el correcto almacenamiento de la información antes de proceder a almacenarla en un sistema de almacenamiento seguro.

6.6. Gestión de la seguridad de las redes

6.6.1. Controles de red

La red de telecomunicaciones de Equiver estará bajo la presente política para evitar ataques, contando con mecanismos de protección, control y monitoreo de red para filtrar y bloquear tráfico no autorizado. SIDECAM contará con la configuración establecida en el documento de Controles de Red.

6.6.2. Seguridad de los servicios de red

Todas las redes de trabajo deben ser monitoreadas con programas adecuados para detectar accesos no deseados o uso inadecuado de la infraestructura.

6.7. Manipulación de los medios

6.7.1. Gestión de los medios extraíbles

Todos los equipos informáticos que manejen o almacenen información de salud, tendrán bloqueados los puertos USB y en su caso lectores de memoria. Así mismo el personal de la organización utilizará los mecanismos institucionales autorizados para la transferencia o compartición de información.

En el caso en el que sea necesario almacenar información de salud en algún equipo o dispositivo específico por algún motivo particular, debe existir previamente una autorización del GSI.

6.7.2. Retirada de medios

Al retirar de funcionamiento cualquier medio de almacenamiento de información de los equipos de cómputo, se realiza un procedimiento para eliminar la información y restaurar el equipo a sus valores de fábrica. Se llevará un registro documental de la baja o reasignación del equipo en cuestión.

6.7.3. Procedimientos de manipulación de la información

Los respaldos del sistema que procesa y administra información de salud se almacenarán directamente en la plataforma segura de nube, siguiendo lo indicado en el documento: Copias de Seguridad de la Información en Salud

6.7.4. Seguridad de la documentación del sistema

La documentación de los sistemas de información será tratada como información sensible, por lo que será almacenada en medios cifrados o sistemas con acceso controlado autorizado y sólo accesibles por personal autorizado por la Dirección o GSI.

6.8. Intercambio de información

6.8.1. Políticas y procedimientos de intercambio de información de salud

Todo intercambio de información será en apego a las Guía de Información publicadas por la autoridad.

6.8.2. Acuerdos de intercambio

Todo intercambio de información será firmado por las partes involucradas especificando exactamente qué información será intercambiada y con qué fin, de acuerdo con el numeral 6.8.1. del presente documento, dicho intercambio será autorizado por la dirección o GSI.

6.8.3. Medios físicos en tránsito

Si un medio donde exista información de salud debe abandonar las instalaciones, esto será notificado al GSI para determinar la procedencia del movimiento y proveer medios de almacenamiento autorizados por la organización, mismos que sólo serán usados por el personal autorizado.

6.8.4. Mensajería electrónica

Actualmente Equiver no utiliza la mensajería electrónica para ningún sistema que administre o procese información de salud, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

6.8.5. Sistemas de información de salud

El sistema SIDECAM únicamente llevará a cabo el intercambio de información a través de los lineamientos y directrices establecidas por la autoridad en salud a través de los mecanismos que para este fin dicha autoridad

publique.

6.9. Servicios de comercio electrónico en salud

6.9.1. Comercio electrónico

Actualmente dentro de Equiver no existen sistemas de comercio electrónico que administre o procese información de salud, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

6.9.2. Transacciones en línea

Actualmente en Equiver no existen sistemas que realizan transacciones de comercio electrónico que administre o procese información de salud, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

6.9.3. Información de salud públicamente disponible

Actualmente en Equiver no existen sistemas que sean de uso público y que administre o procese información de salud, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

6.10. Supervisión

6.10.1. Registros de auditoría

SIDECAM cuenta con el registro de eventos y actividades donde cada vez que un usuario accede, crea, actualiza o guarde información se almacenarán datos que identifiquen el usuario, equipo de cómputo, evento, acción realizada y fecha.

6.10.2. Supervisión del uso del sistema

El registro de información descrito en el numeral anterior, estará disponible para los usuarios autorizados a través de reportes para los fines que determine el GSI o la Dirección.

6.10.3. Protección de la información de los registros

El registro de información descrito en el numeral 6.10.1, estará protegido por perfiles de lectura para evitar su modificación por cualquiera de los usuarios del sistema.

6.10.4. Registros de administración y operación

El registro de información descrito en el numeral 6.10.1 incluye el registro de los eventos relacionados con las actividades de usuarios con perfiles de operación y administración de SIDECAM.

6.10.5. Registro de fallos

Para los fallos (incidencias) ocurridas dentro de la operación del SIDECAM, se mantendrá un registro de las incidencias detectadas y reportadas de acuerdo con el PTI-03 Registro de Fallos y el Manual de Usuario.

6.10.6. Sincronización del reloj

El sistema SIDECAM mantendrá una sincronización de reloj mediante un servidor NTP (Network Time Protocol) a fin de garantizar la homologación del tiempo.

7.Control de Acceso

7.1. Requisitos de control de acceso en salud

7.1.1. Política de control de acceso

El sistema SIDECAM contará con un mecanismo de acceso que sólo permitirá la entrada al personal autorizado y dependiendo de sus funciones específicas, únicamente mostrará la información que le compete.

Los accesos a SIDECAM para el personal de Equiver son autorizados por el GSI quienes incorporarán dicha información como parte del listado de activos a cargo del responsable de dicho acceso.

7.2. Requisitos Gestión de acceso de usuario

7.2.1. Registro de usuario

Los accesos a sistemas que administren o procesen información de salud deben estar documentados de acuerdo con el Registro y Gestión de Privilegios de Usuarios.

SIDECAM cuenta con un módulo que permite el registro controlado de usuarios.

El GSI tendrá usuarios con perfil Administrador para asignar, limitar y restringir usuarios, los cuales estarán registrados en la Relación de Usuarios indicando que cuentan con el perfil mencionado.

El registro de usuarios se lleva de la siguiente manera:

1. El solicitante interno o externo deberá solicitar vía correo electrónico a sidecam@equiver.com.mx el Formato de Solicitud de Alta de Usuario en sistema de información y enviarlo debidamente llenado para su autorización por el mismo medio.
2. Un miembro del SGI, atiende la solicitud de acuerdo con los pasos del Registro de Usuario.
3. Para la Gestión de Privilegios, se asigna el privilegio y rol.
4. Para llevar un control de usuarios se procede a llenar el documento: Relación de usuarios SIDECAM.
5. Por medio del correo sidecam@equiver.com.mx se notifica al solicitante el Alta de usuario y se le notifica.

En caso de ser externo se enviará los usuarios y contraseñas de acuerdo con lo establecido por ambas partes, a las personas responsables que se designe por el cliente para el control y resguardo correspondiente, siempre manteniendo la seguridad de la información. Para el caso de Gobierno o dependencia se realizará por medio de oficio.

Los accesos a sistemas que administren o procesen información de salud deben estar documentados en el listado de activos y ser autorizados por el GSI por medio del formato de asignación de activos.

7.2.2. Gestión de privilegios

El GSI mantendrá actualizado el documento Relación de usuarios SIDECAM y contendrá entre otros, los usuarios y privilegios que posee cada uno dentro de SIDECAM, con el fin de cotejar y validar que efectivamente cumplen con las funciones específicas que le competen al usuario.

7.2.3. Gestión de contraseñas de usuarios

Las contraseñas de SIDECAM serán creadas y administradas considerando las siguientes características:

- Letras mayúsculas (**A** a la **Z**)
- Letras minúsculas (**a** a la **z**)
- Números
- Incluir caracteres especiales (puntos, guion bajo, guion medio, etc.)
- Se deben utilizar al menos 8 caracteres.

- Coincidir con la confirmación

En el manejo de contraseñas se debe tomar en cuenta:

- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de esta.
- No enviar nunca la contraseña por correo electrónico o en un SMS.
- No escribir las contraseñas en archivos sin protección o de los que se desconozca su nivel de seguridad.

7.2.4. Revisión de los derechos de acceso de usuario

Se harán revisiones semestrales en las que se revise que los accesos provistos a SIDECAM estén actualizados y correspondan a la operación vigente de la organización. Dicha revisión la llevará a cabo el GSI constatando que no haya usuarios con privilegios adicionales ni usuarios inactivos o que ya fueron cesados.

7.3. Responsabilidades de usuario

7.3.1. Uso de contraseñas

Los usuarios de SIDECAM tendrá conocimiento de las recomendaciones establecidas por la presente política de seguridad, para tal fin, la dirección dará a conocer esta información de forma regular y haciendo hincapié en la responsabilidad del manejo de estas.

7.3.2. Equipo de usuario desatendido

Los equipos de cómputo desde los que se accede a SIDECAM o manejen información de salud, deben bloquearse por el usuario al abandonar la estación de trabajo para evitar accesos no deseados. Si permanecen desatendidos por más de cinco 5 minutos, se deberán bloquear de forma automática y solicitar contraseña.

7.3.3. Política de puesto de trabajo despejado y pantalla limpia

Los espacios de trabajo dentro de Equiver cumplirán con lo siguiente:

- No debe existir a la vista o a la mano documentos con información sensible o de salud.
- No debe haber a la vista o a la mano dispositivos de almacenamiento que contengan información sensible o de salud sin la adecuada supervisión.
- Los escritorios y áreas de trabajo deberán estar libres de alimentos.
- El área de trabajo debe estar despejada, sólo con el material que es requerido para la actividad que se desempeña.

7.4. Control de acceso a la red

7.4.1. Uso Política de uso de los servicios en red

El servicio de red será proporcionado a todo usuario autorizado que cuenta con una computadora y hace uso de la red interna de Equiver, tomando en cuenta lo siguiente:

- El GSI se reserva el derecho de bloquear sitios de Internet que no cumplan con fines laborales de la organización.
- El GSI se reserva el derecho de restringir o negar servicio de red en equipos que se detecte algún abuso o provoquen interrupciones.
- Se restringirán los servicios de red aquellos usuarios que intentan violar la seguridad de cualquier equipo.
- No está permitido el uso de la red para actividades recreativas (juegos, descargas, streaming, etc.).
- Está prohibido instalar y habilitar en los equipos de cómputo servicios como: servidores web, FTP, DHCP, DNS, IRC, correo electrónico, proxy o instalar una dirección IP fija en una computadora sin la autorización correspondiente.
- Es responsable el usuario por los sitios que visite en Internet.

7.4.2. Autenticación de usuario para conexiones externas

Los usuarios o terceros que se conecten a la infraestructura de red de Equiver y dicha conexión impliquen el acceso a información confidencial o de salud, deberán hacerlo a través de los mecanismos autorizados por el GSI, previa autorización.

Solo por motivos especiales se podrá acceder vía remota a la red, estos motivos serán para soporte o configuración de alguna de las infraestructuras de la empresa. Para poder acceder se deberán tomar en cuenta los siguientes puntos:

- Equiver autoriza como servicios de conexiones externas: VPN, DNS, escritorios remotos y aplicaciones para conexión remota.
- Cualquier conexión será previamente justificada y autorizada por el GSI.
- La conexión será restringida a ciertos equipos dentro de un tiempo determinado, mientras se efectúen las labores de soporte o mantenimiento.
- Todas las conexiones remotas serán monitoreadas mientras estén activas.

7.4.3. Identificación de los equipos en las redes

El personal de TI controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de dirección IP y portal cautivo para la conexión inalámbrica.

7.4.4. Protección de los puertos de diagnóstico remoto y protección de los puertos de configuración

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, Servidores y equipos de usuario final, estarán restringido a los administradores de red o servidores.

Así mismo, únicamente serán habilitados aquellos puertos que el propio SIDECAM requiera para brindar los servicios para los cuales se haya construido.

7.4.5. Segregación de las redes

El sistema SIDECAM será implementado de manera independiente de la red local de Equiver, específicamente en servidores dedicados para dicho fin se haya habilitado.

7.4.6. Control de la conexión a la red

Dentro de la red de datos de Equiver, se restringirá mediante el antivirus instalado en cada equipo el acceso a sitios no seguros, sitios no permitidos, descargas no autorizadas, protección contra ataques y tráfico entrante sospechoso.

El GSI podrá determinar establecer excepciones de acuerdo con las funciones de usuarios específicos, sin comprometer la seguridad de la información.

7.4.7. Control de enrutamiento (routing) de red

Las conexiones no seguras a los servicios de red pueden afectar a toda la organización, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

Adicionalmente se utilizarán métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.

7.5. Control de acceso al sistema operativo

7.5.1. Procedimientos seguros de inicio de sesión

El acceso al sistema operativo de todos los equipos de cómputo estará protegido mediante un inicio seguro de sesión mediante usuario y contraseña, considerando lo siguiente:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- Validar los datos de acceso, una vez que se han gestionado todos los datos de entrada.
- No mostrar las contraseñas escritas.

7.5.2. Identificación y autenticación de usuario

Los nombres de usuario para las cuentas de acceso a SIDECAM serán únicos para su uso personal y exclusivo, de tal forma que puedan ser identificados claramente. Por otro lado, los equipos de cómputo deberán tener como parte de su nomenclatura el nombre del usuario responsable, indicando nombre y apellido.

7.5.3. Sistema de gestión de contraseñas

De acuerdo con los criterios establecidos para la generación y administración de contraseñas, los equipos de cómputo deberán apegarse a dichos criterios, tal como se establece en el numeral 7.2.3 del presente documento.

7.5.4. Uso de los recursos del sistema

Los equipos de cómputo contarán con restricciones para el uso o instalación de software, solo el personal autorizado podrá instalar y determinar qué software es necesario para el usuario. Si requiere software adicional, éste deberá ser aprobado por la dirección y el GSI.

7.5.5. Desconexión automática de sesión

Los equipos de cómputo después de cinco minutos de inactividad se bloqueará la sesión de usuario, requiriendo nuevamente el ingreso de la contraseña de acceso.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar parcial o totalmente su puesto de trabajo por un periodo indefinido.

7.5.6. Limitación del tiempo de conexión

El sistema SIDECAM contabilizará el tiempo de inactividad de un usuario en sesión, mismo que al cumplirse un tiempo determinado establecido de dicha inactividad, el sistema cerrará automáticamente la sesión.

7.6. Control de acceso al sistema operativo

7.6.1. Restricción de acceso a la información

El acceso al sistema SIDECAM, respaldos del sistema, documentación de procesos sensibles, información compartida o inventarios será restringido al personal autorizado o que en sus funciones laborales sea necesario el uso de estos activos.

Estos sistemas y la información de trabajo estarán protegidos mecanismos de restricción de acceso.

7.6.2. Aislamiento de sistemas sensibles

Los sistemas que administren o procesen información de salud permanecerán aislados en un entorno informático propio, compartiendo recursos con otros sistemas de aplicaciones autorizadas.

7.7. Equipos de cómputo portátil y teletrabajo

7.7.1. Equipos de cómputo portátil y comunicaciones móviles

Todos los equipos de cómputo móviles (laptops) que administren o procesen información de salud, estarán asignados a un área específica y serán trasladados únicamente bajo la autorización correspondiente del GSI.

7.7.2. Teletrabajo

Actualmente SIDECAM no cuenta con funcionalidades relacionadas con telemedicina o telesalud, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

8.1. Requisitos de seguridad de los sistemas de información

8.1.1. Análisis y especificación de los requisitos de seguridad

Como parte de la implementación de SIDECAM, éste se pegará a los siguientes controles de seguridad:

- Contará con un entorno dedicado para su ejecución.
- Los accesos a servidores web, de base de datos, FTP, SFTP, entre otros, deberán estar autorizados por el GSI.
- Existirán diferentes roles de usuario y niveles de acceso dependiendo de las responsabilidades y funciones que tenga cada usuario.
- Contará con un registro de auditoría que permita identificar cada acción efectuada y el usuario que la llevó a cabo, con independencia si se trata de un usuario operativo o administrador del sistema. Dicha información estará disponible para los usuarios especializados.
- Contará con un sistema de acceso seguro con el que se pueda proteger la información que albergan.
- Todos los nombres de usuario del sistema serán únicos.
- Los mecanismos para establecer contraseñas funcionarán en apego a la presente política de seguridad.
- Las sesiones dentro de los sistemas serán cerradas después de un periodo de inactividad.
- La información que se use en ambientes de desarrollo y pruebas será diferente a la que exista en el ambiente de producción para proteger la confidencialidad de los datos.

8.2. Procesamiento Correcto en Aplicaciones

8.2.1. Identificación única de sujetos de atención

Todos los sistemas que administren o procesen información de salud deben identificar a los sujetos de atención (pacientes) de una identificación única, este identificador puede ser interno o usar elementos como la CURP de identificador. Si un usuario es capturado dos veces, el sistema debe ser capaz de identificar la duplicidad y fusionar los registros previos, para realizar lo anterior se debe consultar dicha sección en el Manual de Usuario SIDECAM.

8.2.2. Validación de los datos de entrada

SIDECAM validará la información por almacenar, verificando que los datos indispensables sean capturados, que haya coherencia en la información capturada de acuerdo con las guías aplicables.

8.2.3. Control de procesamiento interno

SIDECAM validará la información después de ser capturada y antes de ser procesada, para detectar si la información es coherente mostrando una pantalla de confirmación.

8.2.4. Integridad de los mensajes

SIDECAM, para mantener la integridad de los mensajes genera los archivos de intercambio de acuerdo con las guías de cifrado proporcionadas por la autoridad de Salud. Para realizar el procedimiento se debe consultar el Manual de Usuario.

8.2.5. Validación de los datos de salida

Los sistemas que administren o procesen información de salud deben mostrar la información del sujeto de atención o pacientes cada vez que se vaya a actualizar o modificar, con la finalidad de garantizar que el tratamiento de la información almacenada sea el adecuado, con el archivo generado y validado por la autoridad cumpliendo con las guías aplicables.

8.3. Controles criptográficos

8.3.1. Política de uso de los controles criptográficos y gestión de claves

Los controles criptográficos que se llegasen a utilizar en SIDECAM se mantendrán bajo resguardo del GSI, los cuales serán responsables del uso y almacenamiento de estos.

8.3.2. Gestión de claves

Las claves que se usen en SIDECAM serán gestionadas por el GSI y deberán:

- Renovar las claves frecuentemente.
- Usar claves diferentes para servicios diferentes (autenticación, transmisión, almacenamiento, etc.) con el fin de minimizar la exposición de las claves.
- Asignar claves diferentes a cada persona o grupo que acceden al sistema, de tal manera que sólo las personas autorizadas tengan acceso a determinada información.
- Las claves que por alguna razón se vuelven no seguras o aquellas que ya no son usadas por algún usuario serán eliminadas.
- La distribución de las claves para los usuarios debe ser de forma manual, evitando proporcionar la información por medios digitales.

8.4. Seguridad de los archivos de sistema

8.4.1. Control del software en explotación

La administración de los servidores donde se ejecuten las aplicaciones de información de salud como SIDECAM la llevará a cabo el personal que para este fin autorice el GSI o la dirección, aun cuando sea un proveedor encargado para esa función. Si se requiere que alguien más acceda, como equipos de desarrollo y externos deberán poseer una autorización por parte del GSI.

En los servidores solo existirán las aplicaciones estrictamente necesarias para su funcionamiento, queda prohibido instalar aplicaciones adicionales sin la autorización de la dirección y/o el GSI. Si se requiere una aplicación o programa adicional ésta deberá contar con la autorización formal por parte del GSI.

El GSI llevará a cabo una supervisión cada determinado tiempo del software que está instalado y determinar si es el correcto y no hubo algún cambio.

8.4.2. Protección de los datos de prueba del sistema

Queda prohibido el uso de información real en cualquier ambiente de pruebas o desarrollo. Se deberán usar datos ficticios o en su defecto una mezcla de información siempre y cuando se asegure que ningún dato es real.

8.4.3. Control de acceso al código fuente de los programas

El acceso al código fuente de SIDECAM está restringido sólo al personal autorizado, así como los equipos de desarrollo o el equipo de TI. Estos firmarán acuerdos de confidencialidad, haciéndose responsables del resguardo del código y su autoría.

El código implementado en el servidor deberá tener protecciones para evitar la modificación de este, puede ser que esté previamente compilado o en su defecto accesos restringidos a las carpetas de producción.

8.5. Seguridad en los procesos de desarrollo y soporte

8.5.1. Procedimientos de control de cambios

Cualquier modificación que se realice a SIDECAM será autorizada por la dirección y/o el GSI, después de haber aprobado y comprobado el cambio en un ambiente de pruebas.

Todos los cambios deberán ser autorizados por medio del Procedimiento Gestión de Cambios, el cual incluirá entre otros:

- Nombre del sistema
- Nuevas funcionalidades y/o errores corregidos
- Fecha de liberación
- Observaciones

Si existen detalles dentro de la revisión previa, el cambio no será aprobado.

8.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Cualquier modificación que haya sido implementada en producción debe ser revisada por el personal operativo y validada por el GSI, las pruebas que se llevarán a cabo serán de todas las funciones para asegurar que el sistema trabaja completamente. Se usará Jira como medio de validación siguiendo el numeral 8.5.1, el cual debe incluir:

- Nombre del sistema
- Número de versión.
- Funcionalidades probadas
- Errores encontrados
- Fecha de revisión
- Observaciones

8.5.3. Restricciones a los cambios en los paquetes de software

Los accesos a los ambientes productivos serán restringidos y la instalación o cualquier modificación que se realice en alguna aplicación debe ir autorizado por la dirección y/o el GSI quienes podrán brindar accesos temporales.

Todo cambio dentro de SIDECAM debe estar plenamente justificado, y se deberá realizar de acuerdo con el numeral 8.5.1

8.5.4. Fugas de información

El personal que maneja información de salud firmará acuerdos de confidencialidad, conocerá los aspectos de seguridad que le competen y las sanciones correspondientes por incumplimiento u omisión.

8.5.5. Externalización del desarrollo de software

Para los proyectos de desarrollo de software que requieran la contratación de terceros para su ejecución, Equiver asignará un líder de proyecto quien será el encargado de supervisar de manera continua los trabajos realizados por externos.

8.6. Gestión de las vulnerabilidades técnicas

8.6.1. Control de las vulnerabilidades técnicas

Equiver buscará asegurarse que SIDECAM no tenga vulnerabilidades que puedan comprometer la información y la integridad del sistema. Para ello usará sistemas de escaneo que brinden informes de seguridad que permitan corregir y detectar posibles fallas, las cuales deberán ser corregidas de acuerdo al nivel de criticidad descritos dichos informes.

9.Gestión de Incidentes en la Seguridad de la Información

9.1. Notificación de eventos y puntos débiles de seguridad de la información

9.1.1. Notificación de eventos de seguridad de la información

SIDECAM contará con la dirección de correo electrónico sidecam@equiver.com.mx en el cual los usuarios podrán reportar cualquier falla o posibles acontecimientos de seguridad.

9.1.2. Notificación de puntos débiles de seguridad

Todo el personal interno y externo de Equiver conocerá la política de seguridad de la información y según corresponda, firmará acuerdos de confidencialidad donde se incluye la responsabilidad de notificar las observaciones o sospechas de puntos débiles de seguridad.

9.2. Gestión de incidentes y mejoras de seguridad de la información

9.2.1. Responsabilidades y procedimientos

Los encargados de la administración de SIDECAM usarán los canales de comunicación de incidencias para detectar y solucionar los problemas detectados en el sistema.

Al detectar un incidente se realizará lo siguiente:

- El usuario envía un correo electrónico a sidecam@equiver.com.mx con la descripción del incidente.
- Se determinará la gravedad del incidente.
- Se verificará el suceso dentro del sistema.
- Si el incidente requiere de análisis por parte del equipo de desarrollo se turnará con la información del incidente.
- Dependiendo de la respuesta del equipo de desarrollo se notificará al usuario para mantenerlo informado.
- Si el equipo de desarrollo ha solucionado el incidente, se da por cerrado.
- Si la solución requiere de alguna modificación de código dentro del sistema el encargado de la administración gestionará los formatos de cambio y pruebas del sistema para posteriormente liberar una nueva versión con las correcciones necesarias.
- Después se deberá verificar que se haya dado solución al incidente y se da por cerrado.
- En cada caso, cuando la solución sea efectiva se debe notificar al usuario de la solución y se deberá llenar el formato de soporte con las observaciones y soluciones implementadas.

9.2.2. Aprendizaje de los incidentes

A partir de los incidentes reportados y con el PTI-03 Registro de Fallos, se generará una base de conocimiento para buscar en ella posibles soluciones cuando se presentan incidencias. Dicha base se lleva dentro de las aplicaciones autorizadas y consolidará información relevante del incidente y a la solución.

La información estará disponible para el GSI, los encargados de brindar soporte y aquellos que para este fin determine el GSI o la Dirección.

9.2.3. Recopilación de evidencias

La recopilación de incidentes quedará documentado dentro de la aplicación de gestión de incidencias, siguiendo con el PTI-03 Registro de Fallos y en caso de aplicar el correo electrónico a sidecam@equiver.com.mx, conformando por un expediente con los detalles técnicos y/o correos electrónicos y/o capturas de pantalla y/o registros del sistema entre otros.

10.Gestión de Incidentes en la Seguridad de la Información

10.1. Gestión de la continuidad del negocio

10.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

En el caso que SIDECAM dejase de funcionar por algún motivo, el GSI será el encargado de identificar el motivo que lo originó y el posible daño producido para permitir recuperar en el menor tiempo posible el activo afectado. Para documentar dicho evento el GSI llevará a cabo el siguiente procedimiento:

- Registro de falla
- Notificación al proveedor o área responsable
- El proveedor o área responsable lleva a cabo las acciones correctivas
- El área usuaria valida el funcionamiento de los servicios
- Se notifica a los usuarios del restablecimiento del servicio

10.1.2. Continuidad del negocio y evaluación de riesgos

Los sistemas de información son susceptibles a contingencias que ponen en riesgo la información y la operación. A partir del análisis de riesgos realizado por el GSI, se identificaron los siguientes factores de riesgo:

- Falla en servidores centrales.
- Desastre natural.
- Centro de datos.
- Falla en telecomunicaciones.
- Falla en el suministro de energía eléctrica.
- Ataques informáticos.
- Error humano.

En caso de que el GSI identifique algún otro factor que ponga en riesgo la continuidad operativa de SIDECAM lo hará de conocimiento de la dirección y/o de los usuarios involucrados.

10.1.3. Continuidad desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Con el fin de garantizar la continuidad operativa del sistema SIDECAM, el GSI definirá y documentará un plan de contingencia, mediante el cual ante alguna posible falla del sistema se buscará dar continuidad operativa a través de medios alternativos a aquellos procesos y funcionalidades que de manera productiva son proveídas por SIEDECAM.

El plan de contingencia será aprobado por la dirección y podrá revisarse cuando ésta así lo determine conveniente.

10.1.4. Marco de referencia para la planificación de la continuidad del negocio

Para Equiver, dentro del alcance de la presente política de seguridad, el marco de referencia para llevar a cabo una planeación adecuada que asegure la continuidad operativa de los procesos asociados con el sistema SIDECAM se conforma de lo siguiente:

- Mantener identificados los activos de información.
- A cada activo de información asociar un responsable.

- Documentar los riesgos e impactos relacionados con la seguridad de la información.
- Establecer planes de solución o mitigación de los riesgos identificados.
- Establecer niveles de servicio con los terceros cuyos servicios prestados se relacionen con la continuidad operativa de SIDECAM.

10.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

De acuerdo con el plan de contingencia referido en el numeral 10.1.1 del presente documento, el GSI llevará a cabo de manera programada pruebas controladas mediante las cuales se valide la vigencia y aplicabilidad de dicho plan.

En caso de que dicha prueba, resulte en la necesidad de actualizar el propio plan, esto deberá llevarse a cabo por el propio GSI. Así mismo, en caso de que se identifiquen fallas o áreas de oportunidad en los procesos productivos que se están llevando a cabo, se deberán aplicar las acciones correctivas o preventivas correspondientes a fin de mitigar los riesgos o garantizar que el plan de contingencia tendrá la efectividad esperada.

11.Cumplimiento

11.1. Cumplimiento de los requisitos legales

11.1.1. Identificación de la legislación aplicable

De acuerdo con el alcance a las disposiciones jurídicas aplicables y el alcance del propio sistema SIDECAM, Equiver establece como el marco normativo, legal y jurídico aplicable las siguientes disposiciones:

- NOM-024-SSA3-2012, Sistemas de Información de Registro Electrónico para la Salud.
- LFTAIPG, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- LFPDPPP, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley General de Salud.
- NOM-004-SSA2-2012 con las guías aplicables.

11.1.2. Derechos de propiedad intelectual (IPR)

En cumplimiento y garantía de la propiedad intelectual de SIDECAM y demás activos de información relacionados, Equiver contará con la siguiente documentación o información:

- Registro ante el Instituto Mexicano de la Propiedad Intelectual del sistema.
- Uso exclusivo de software con su respectivo licenciamiento de uso.

El GSI mantendrá un listado actualizado con el Inventario de Activos, indicando sí cuenta con las licencias de software de los equipos de cómputo de la empresa, utilidades de ofimática, sistemas operativos, antivirus y demás aplicativos que pudieran usarse en la operación.

11.1.3. Protección de los documentos de la organización

La dirección será la encargada brindar los mecanismos para resguardar la información y documentación crítica de la organización, incluyendo la información de salud. Estos medios garantizarán la protección contra la pérdida o destrucción de la información.

Los medios para resguardo podrán incluir cajas fuertes, digitalización de documentos críticos, sistemas de seguridad, pólizas de seguro, entre otros.

11.1.4. Protección de datos y privacidad de la información de carácter personal

Conforme a la legislación aplicable en materia de protección de datos y privacidad de la información, dentro del sistema SIDECAM se encontrará disponible para consulta la política de manejo y uso de la información personal.

11.1.5. Prevención del uso indebido de recursos de tratamiento de la información y regulación de los controles criptográficos

Conforme a la legislación aplicable en materia de protección de datos y privacidad de la información, dentro del sistema SIDECAM, Equiver llevará a cabo la difusión correspondiente a través de diversos medios, tales como correo electrónico, llamadas telefónicas, medios de difusión impresos y aquellos que la dirección o el GSI determinen.

11.1.6. Regulación de los controles criptográficos

Actualmente en México no hay legislación que regule o especifique el uso de controles criptográficos, motivo por el cual no se establece ningún control de seguridad asociado a éste rubro.

11.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

11.2.1. Cumplimiento de las políticas y normas de seguridad

La dirección y el GSI se asegurará que la presente política de seguridad se esté cumpliendo a través de revisiones, supervisiones o auditorías programadas. El periodo entre una revisión y otra lo definirá el GSI.

11.2.2. Comprobación del cumplimiento técnico

La dirección y el personal que para este fin se defina, se asegurará que SIDECAM cumpla con los requisitos técnicos y normativos establecidos principalmente en la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de Registro Electrónico para la Salud. Intercambio de información en salud.

En este sentido, se utilizarán como referencia los siguientes aspectos:

- Implementación de los datos mínimos de identificación de personas.
- Implementación de catálogos fundamentales.
- Cumplimiento de las guías de intercambio de información aplicables.
- Cumplimiento de los controles de seguridad aplicables para la implementación del Sistema de Gestión de Seguridad de la Información.

El periodo entre una revisión y otra lo definirá el GSI.

11.3. Consideraciones sobre las auditorías de los sistemas de información en salud

11.3.1. Controles de auditoría de los sistemas de información

La dirección y el GSI realizarán las auditorías pertinentes sobre el funcionamiento de SIDECAM, con el fin de detectar posibles errores de seguridad en accesos o mal uso de los usuarios. Se utilizarán las herramientas de monitoreo que el GSI determine para verificar que no existan vulnerabilidades o factores que no se hayan detectado.

El periodo entre una revisión y otra lo definirá el GSI.

11.3.2. Protección de las herramientas de auditoría de los sistemas de información

El uso de las herramientas de auditoría y aplicaciones de monitoreo y escaneo quedan estrictamente restringidas para uso y manejo del GSI, quienes se harán responsables del resguardo y protección de estas.