Equipo y Tecnología para el cuidado de la vida

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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 una vez cada 6 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

1. 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. Además de evaluar constantemente la infraestructura de la organización, así como realizar el seguimiento adecuado de las actividades.

La Dirección general designará a una persona encargada 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: encargado de tecnologías de la información 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. • 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. • 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.
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: Director de Operaciones 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 la 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.

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 explícitamente 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, dentro de las que se encuentran:

- **Dirección de operaciones**:
    - Dar a conocer la política de seguridad de la información, así como las sanciones por omisión o incumplimiento.
    - Capacitar al personal en el sistema de de sistema de gestión de la seguridad de la información (SGSI).
    - Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del SGSI
    - Aplicar las medidas y controles de seguridad correspondientes a las diferentes áreas operativas.
    - Monitorear a las áreas operativas para detectar problemáticas y mejoras de seguridad.
    - Gestionar recursos para el cumplimiento del SGSI.
    - Elaborar informes de operación y cumplimiento de funciones tanto del personal como proveedores externos.
    - Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI

- **Dirección de cuentas clave**:
    - Verificar el cumplimiento de las normativas de seguridad en los

sistemas de información de salud.

- Analizar el funcionamiento de los sistemas de información y brindar soporte en caso de posibles fallos.
- Gestionar los usuarios y roles en los sistemas de información.
- Coordinar el proceso de cambio y mejoras dentro de los sistemas de información.
- Elaborar informes y estadísticas de los sistemas de información.
- Desarrollo y atención de auditorías del sistema.

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 éste fin se haya establecido, mismo que contendrá:

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

2.1.5 Acuerdos de confidencialidad

Todo el personal que labora en Equiver firmará un documento 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.

2.1.6 Contacto con las autoridades

Debido a la naturaleza actual de las tecnologías de información y su evolución constante, el GSI estará en contacto con entidades externas enfocadas o relacionadas con la seguridad de la información para tomar nota de posibles cambios en legislación o procedimientos de seguridad.

Este contacto podrá ser a través de consultas formales, participación en eventos (congresos, cursos, etc.) cuya temática sea la seguridad de la información o a través de medios electrónicos, dentro de los cuales se considerarán las páginas en internet, redes sociales o correo electrónico.

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.

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

De acuerdo con el análisis que realice el GSI, se identificarán los riesgos que impliquen las personas ajenas a la empresa Equiver, se documentará 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 anexo.

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

Todos los usuarios internos, así como los terceros relacionados con el acceso, procesamiento, comunicación o gestión de alguno de los activos de información en salud, estarán comprometidos con el cumplimiento de la política de seguridad de la información, así como las sanciones asociadas que haya establecido Equiver.

Dicho compromiso será formalizado a través del respectivo contrato de servicios 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 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 a 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.

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 que se consideren de alta prioridad.

3.2 Clasificación de la información de salud

3.2.1 Lineamientos de clasificación

Equiver en la relación 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, valor, 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 la misma, 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 y externo deberá conocer sus funciones y responsabilidades de cara a la seguridad de la información antes y durante el ejercicio de sus funciones.

Para dar cumplimiento a lo anterior, todo aquel que 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 correspondiente y éste deberá firmar de conocimiento.

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 las mismas.

4.1.2 Investigación de antecedentes

Las áreas que dentro de Equiver se encarguen de llevar a cabo contratación de personal interno, así como de terceros, 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:

- 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, así como

de terceros, deberá mantener los registros de dicha investigación.

4.1.3 Términos y condiciones de empleo

El personal interno de Equiver, los proveedores, contratistas y terceros que procesan 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 las mismas.

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

La Dirección General 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 periódica, de manera que se mantenga actualizado y

comprometido con la seguridad de la información.

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

- Correos electrónicos
- Videos institucionales
- Pláticas de seguridad de la información
- Carteles o trípticos en materia de seguridad

4.2.3 Proceso disciplinario

Las políticas y lineamientos de Seguridad Informática 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 evaluará el impacto, a partir del cual 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 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 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, la Dirección 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 área de seguridad informática 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 documento de responsabilidad y descripción 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 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 evaluación del riesgo de seguridad y 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 guardias de seguridad y personal 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

En las áreas de acceso público se tendrán controles específicos de seguridad, mismos que todo visitante o personal externo debe acatar:

a) Estar ubicados en una sola área controlada y vigilada.

b) Siempre que sea posible, dichas áreas estarán fuera del perímetro de cualquier área de seguridad. Si esto no fuera posible, debe ubicarse el control de acceso de forma tal que se reciba a los visitantes antes de que éstos tengan acceso a las instalaciones.

c) Confirmar y registrar efectivamente las identidades de los visitantes, las organizaciones a las que representan, y el objetivo de su visita antes de ser admitidos.

d) Registrar las fechas y horarios de entrada y salida.

e) Proporcionar a los visitantes gafetes distintivos, los cuales deben portar durante su visita.

f) Garantizar que los visitantes estén bajo observación y sean supervisados durante su visita, en función de los riesgos. Y en todo caso deben estar acompañados de la persona a quien visiten.

g) Minimizar el acceso de los visitantes, principalmente a las áreas de seguridad.

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 la misma, 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, 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 la dirección antes de ser aplicados en ambientes de producción. Dichas modificaciones serán formalizadas en un documento creado específicamente para tal fin.

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 a las labores específicas de los principales usuarios: administrador, operador y/o cliente.

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 que manifieste claramente sus actividades y alcances.

Así mismo, serán documentados los controles aplicables a los activos de información a los que tengan acceso los terceros.

6.2.2. Supervisión y revisión de los servicios prestados por terceros

Los servicios prestados por terceras partes serán monitoreados de acuerdo a los controles de seguridad de la información existentes y criticidad de sus funciones. Se plasmará en un documento el cumplimiento de los servicios proporcionados y éste será aprobado por el GSI.

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 de la dirección o el GSI, tomando en cuenta los controles, el impacto y la criticidad de los procesos involucrados.

6.3. Gestión de la provisión de servicios por terceros

6.3.1. Gestión de capacidades

El sistema SIDECAM será analizado periódicamente de acuerdo a 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 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 por medio de un formato destinado para tal efecto y el formato deberá contener los pormenores del cambio o actualización.

Una vez que hayan sido probados los sistemas, se debe llenar el formato con las observaciones y hallazgos, si las pruebas son satisfactorias deben ser aprobadas por el grupo de seguridad de la información y 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.

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. 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 políticas de seguridad para evitar ataques. Los sistemas de firewall serán implementados para filtrar y bloquear tráfico de red que no sea apto para las funciones dentro de la organización.

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.

Los recursos y archivos compartidos serán escaneados y protegidos contra amenazas de código malicioso.

En las carpetas compartidas no habrá información sensible de salud.

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.

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 de la dirección y el GSI. La autorización será por escrito especificando el motivo y el uso que se dará dentro de la organización.

Nunca se extraerá información de salud para fines ajenos a los establecidos por la organización.

En el caso en el que sea necesario almacenar información de salud por algún motivo particular, se debe almacenar siempre discos duros y USBs corporativos debidamente protegidos y con las medidas de seguridad para evitar algún daño a la información o acceso de personal no autorizado.

6.7.2. Retirada de medios

Al retirar de funcionamiento cualquier medio de almacenamiento de información deben ser evaluados por el área de TI para asegurar que la información contenida en el medio ya no es requerida, de ser así, se hará el respaldo, de lo contrario se eliminará de forma segura.

Si la información o el medio de almacenamiento ha dejado de funcionar, se procederá a la des habilitación o destrucción total a fin de asegurar que no podrá ser accesible por alguien más.

Se formalizará en el documento correspondiente que el medio fue retirado correctamente y en su caso la información fue destruida de forma correcta o respaldada si así se requiere.

6.7.3. Procedimientos de manipulación de la información

La información de salud será almacenada en medios seguros de tal forma que no sea accesible por terceros.

Los respaldos de sistemas o archivos que procesan y administran información de salud se resguardarán en medios seguros, sólo accesibles por personal autorizado por la dirección.

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 y sólo accesibles por personal autorizado por la dirección.

6.8. Intercambio de información

6.8.1. Políticas y procedimientos de intercambio de información de salud

Todo intercambio de información será formalizado y autorizado por la dirección o el GSI, debe apegarse a las normas de seguridad de la información de salud y la presente política de seguridad.

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

El sistema SIDECAM cuenta con un 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, serán protegidos para evitar su modificación por cualquiera de los usuarios del sistema o administradores del

mismo.

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 ocurridos dentro de la operación del SIDECAM, se mantendrá un registro de las incidencias detectadas y reportadas, dicho registro deberá formar parte del expediente documental a cargo del GSI.

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 serán 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 en el listado de activos y ser autorizados por el grupo de seguridad de la información por medio de un formato de alta de usuarios, el cual podrá firmarse por el GSI.

7.2.2. Gestión de privilegios

El GSI mantendrá actualizada una relación que contenga los usuarios y privilegios que posee cada uno dentro de SIDECAM, con el fin de cotejar y revisar periódicamente 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:

- Se deben utilizar al menos 8 caracteres.
- Se debe utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- Letras mayúsculas, de la A a la Z.
- Letras minúsculas, de la a a la z.
- Incluir símbolos (puntos, guion bajo, guion medio, etc.).

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 la misma.
- 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 cuando así lo determine el GSI, para la inspección de la integridad de datos de usuarios y perfiles en SIDECAM.

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. Equipo 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 implique 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, 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 dentro del centro de datos que 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 el acceso a:

- Descarga de archivos de sitios peer to peer.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma

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 los mismos.

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.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han gestionado todos los datos de entrada.
- No mostrar las contraseñas escritas.
- No transmitir las contraseñas en texto plano.

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 deberán estar protegidos con medios de seguridad tales como:

- Discos duros cifrados.
- Sistemas con accesos mediante nombre de usuario y contraseña.
- Información bajo llave, caja fuerte o instalaciones con controles físicos 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. Requisitos de seguridad de los sistemas de información

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 forma 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.

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 y que cumpla con criterios como longitud y tipo de dato.

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 o está corrupta respecto de los datos esperados.

8.2.4. Integridad de los mensajes

Actualmente no existen sistemas de información que utilicen envío de mensajes por ningún medio, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

8.2.5. Validación de los datos de salida

Los sistemas que administren o procesen información de salud deben mostrar la información de los sujeto de atención o pacientes cada vez que esta se vaya actualizar o modificar, con la finalidad de garantizar que el tratamiento de la información almacenada sea el adecuado. Debe mostrar los datos generales como nombre y CURP o en su defecto el identificador que utilice el sistema para el sujeto de atención o paciente.

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 los mismos.

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, aún 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 del mismo, 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 de un formato de cambios, el cual incluirá:

- Nombre del sistema
- Número de versión.
- Nuevas funcionalidades y/o errores corregidos
- Análisis de riesgo
- Acciones específicas para corregir los posibles inconvenientes
- Fecha de liberación
- Observaciones
- Firmas de aprobación

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 un formato de validación el cual debe incluir:

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

Si existen detalles dentro de la revisión el cambio deberá ser desechado y se tendrá que regresar a una versión previa.

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 entregar un análisis de riesgo y las acciones específicas para corregir los posibles inconvenientes que pudieran presentarse. Se deberá usar el formato de cambios para su autorización, descrito en el numeral 8.5.2.

8.5.4. Fugas de información

Equiver para asegurarse que SIDECAM no tenga fugas de información, usará sistemas de escaneo que brinden informes de seguridad, deberán ejecutarse y evaluarse a periodos definidos por el GSI.

Así mismo, 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

Equiver tendrá el control sobre el personal y los equipos de desarrollo externos, gestionando los accesos a los servidores de producción, así como reuniéndose periódicamente para llevar el control de los proyectos y avances.

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 una sección de contacto donde se muestran los datos necesarios para la notificación de sucesos relacionados con la operación del sistema y 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 entre otros aspectos se estipulará la importancia de dar a conocer posibles vulnerabilidades en la seguridad de la empresa. En dichos acuerdos se incluye la responsabilidad de notificar las observaciones o sospechas de puntos débiles.

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 los sistemas.

Al detectar un incidente se realizará lo siguiente:

- Llenar el formato de soporte con las observaciones del usuario.
- 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 formatos de soporte, se generará una base de conocimiento para buscar en ella posibles soluciones cuando se presentan incidencias. Cada formato se almacenará junto con la documentación del incidente y archivos referentes a la solución (correos electrónicos, capturas de pantalla, documentos descriptivos, etc.).

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

9.2.3. Recopilación de evidencias

Cada incidente de seguridad debe estar documentado en un expediente con los detalles técnicos, correos electrónicos, capturas de pantalla, registros del sistema entre otros. La información será resguardada y almacenada por el GSI y podrá ser usada para incidentes de seguridad de la información, que impliquen acciones legales.

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 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 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, Del expediente clínico.

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.
- Relación de sesión de derechos de propiedad intelectual por parte de sus áreas de desarrollo de Software y/o proveedores externos.

El GSI mantendrá un listado actualizado con el inventario de 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 dentro de dicho sistema.

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 las mismas.