POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 1.2

Diciembre 2022

Cerrada. Ferrocarril de Cuernavaca 779, interior 501-6.
Col. Ampliación Granada Del. Miguel Hidalgo C.P. 11529, Cd Mx
RFC: IMA170515JEA
Teléfono: |+52 (55) 54502392
office@imagitech.mx
www.imagitech.mx

1. Política de Seguridad

IMAGITECH (la EMPRESA) comprometido con la seguridad de la información crea una política de seguridad para eliminar los riesgos de seguridad de la información en su operación, planteando los detalles que deberá tomar en cuenta, así como los controles que se aplicarán.

La presente política aplica todo el personal de la EMPRESA, incluyendo terceros y los sistemas de comunicaciones utilizados en la operación de la organización.

Entre los sistemas se incluyen las redes de área local, las computadoras personales (PC) y demás sistemas administrativos, el centro de datos, cuarto de telecomunicaciones, el proveedor de servicios de Internet (ISP) y otros proveedores externos.

1.1 Política de seguridad de la información

1.1.1 Documento de política de seguridad de la información

A lo largo del presente documento se establecen los objetivos, criterios, requisitos, estándares y sanciones que aplicará la EMPRESA como parte de la implementación del sistema de gestión de seguridad de la información (**SGSI**).

1.1.2 Revisión de la política de seguridad de la información

La política de seguridad de la información será revisada una vez cada 12 meses o antes si existiera evento importante de seguridad de la información o significativo en los estándares internacionales y 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 seguridad de la información a través de

recomendaciones 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 responsables para supervisar la política de seguridad descrita en el presente documento.

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 la EMPRESA, el GSI estará conformado por:

- ☐ Líder Ejecutivo
- ☐ Líder Tecnológico
- ☐ Líder de Producto

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 IMAGITECH, 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 IMAGITECH 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 IMAGITECH las funciones de seguridad que deberán observar en sus labores, dentro de las que se encuentran las mencionadas en el control anterior.

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 referidos en el numeral 3.1 de la presente política, indicando adicionalmente la información que manejará o con la que estará interactuando.

2.1.5 Acuerdos de confidencialidad

Todo el personal que labora en IMAGITECH 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

En IMAGITECH se cuenta con un directorio de contactos, dentro del cual se listan aquellas

organizaciones o personas que consideran relevantes derivado del uso y manejo de información en salud dentro del sistema de la organización.

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 SGSI mismas que se llevarán a cabo por personal externo cada dos años.

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 IMAGITECH, se documentará e indicarán los controles de seguridad a implantar previo a otorgar acceso a un tercero a la información en salud manejada por IMAGITECH.

2.2.2 Tratamiento de la seguridad en la relación con los clientes

Como parte del tratamiento de la información, IMAGITECH 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 IMAGITECH:

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 IMAGITECH.

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

IMAGITECH generará y mantendrá una relación de los activos de información. Para cada activo, en dicha relación se tendrán los siguientes datos:

- Nombre del activo
- Tipo de activo (lógico/físico)
- Descripción del activo
- Propietario o responsable del activo
- Custodio del activo
- Clasificación 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

IMAGITECH 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 mediante un formato que podrá incluir:
- ☐ Activos que se reciben
- ☐ Condiciones de uso
- ☐ Firma del responsable del activo

3.1.3 Uso aceptable de los activos de Salud

IMAGITECH a través del inventario de activos descrito en los numeral 3.1.1 y 3.1.2. 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

IMAGITECH 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 o baja), tomando en cuenta los criterios que el GSI 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 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 IMAGITECH, 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.

4.1.2 Investigación de antecedentes

El GSI realizará las diligencias correspondientes para conocer los antecedentes de seguridad y laborales del personal candidato a ser contratado incluyendo prestadores de servicios, cuando el Líder Ejecutivo 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 Currículo Vitae, dentro del cual se pueda validar mediante referencias la información plasmada.

- Domicilio
- Verificar referencias de empleos o proyectos anteriores
- El personal contará con el entrenamiento adecuado sobre las políticas y procedimientos de seguridad de la organización.

El GSI deberá mantener los registros de dicha investigación.

4.1.3 Términos y condiciones de empleo

El personal interno de IMAGITECH, 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, deberá 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 IMAGITECH 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 y 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 responsables de procesar información personal de salud, programas de capacitación en función de las necesidades de la empresa. El personal y socios de la empresa, recibirán capacitación periódica, de manera que se mantengan actualizados y comprometidos 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
- Pláticas de seguridad de la información con consultores externos
- Newsletters periódicos con contenido relevante

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 IMAGITECH.

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.
- Suspensión temporal.
- Suspensión definitiva.

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 líder ejecutivo sobre cualquier terminación de contrato de personal o externos.

c) En caso de representar un riesgo significativo para los activos de información de IMAGITECH, el sujeto en cuestión podrá ser llevado fuera de las instalaciones y se le podrá denegar 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 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 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. Áreas Seguras

5.1.1 Perímetro de seguridad física

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.1.2 Controles físicos de entrada

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.1.3 Seguridad de oficinas, despachos e instalaciones

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.1.4 Protección contra las amenazas externas y de origen ambiental

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.1.5 Trabajo en áreas seguras

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.1.6 Áreas de acceso público y de carga y descarga

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.2 Seguridad de los equipos

5.2.1 Emplazamiento y protección de equipos

El equipo de computo 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 móviles como laptops contarán con un candado de seguridad mientras estén en lugares públicos.
b) Los equipos tendrán contraseñas de acceso.
c) El equipo tendrá una directiva de seguridad de autobloqueo de sesión por inactividad.

5.2.2 Instalaciones de suministro

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

5.2.3 Seguridad del cableado

Este control no aplica ya que los empleados de IMAGITECH trabajan de manera remota y no se cuenta con oficina física.

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 documentarán las acciones realizadas. Se realizará anualmente una revisión de todos los equipos de la empresa para remover software no deseado, actualización de software, remoción de archivos que no pertenezcan a la empresa, actualización de antivirus.

5.2.5 Seguridad de los equipos fuera de las instalaciones

Dada que nuestros empleados laboran de manera remota, la provisión y utilización de equipos de la

empresa fuera de las instalaciones queda 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.

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 serán borrados mediante un proceso de formateo de 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 baja operativa de equipos el cual deberá tener los siguientes datos:
  - Fecha
  - Usuario o personal que fungía como responsable
  - Motivo del retiro
  - Características del equipo que se da de baja
  - Firma del encargado de llevar a cabo la baja del equipo
  - Firma de autorización

Si el equipo es reasignado, la nueva persona responsable deberá firmar como nuevo responsable de dicho activo.

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, llenándose 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. Gestión de comunicaciones y operaciones

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 IMAGITECH a través de la Plataforma IMAGITECH 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.

6.1.2 Gestión de cambios

Los cambios y actualizaciones de los sistemas de manejo de la información en salud serán autorizados por los líderes ejecutivo y/o tecnológico antes de ser aplicados en ambientes de producción. Dichas modificaciones serán formalizadas en comunicaciones a través de medios oficiales como correo electrónico o tickets en el sistema de CRM utilizado.

Así mismo, una vez que nuevas funcionalidades sean liberadas, se generará un documento de “Newsletter” para darlo a conocer a los clientes y usuarios de IMAGITECH.

6.1.3 Segregación de tareas

Asociada a la Plataforma IMAGITECH, existirá una matriz de roles y perfiles que acoten las funciones del sistema de acuerdo con las labores específicas de los principales usuarios: administrador, doctor, enfermería y recepción.

6.1.4 Separación de los recursos de desarrollo, prueba y operación

Se contará con un ambiente de pruebas y desarrollo, separados del ambiente productivo de la Plataforma IMAGITECH.

6.2 Gestión de la provisión de servicios por terceros

6.2.1 Provisión de servicios

Los proveedores al servicio de IMAGITECH 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 con 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.

6.3Gestión de la provisión de servicios por terceros

6.3.1 Gestión de capacidades

La Plataforma IMAGITECH será analizada periódicamente haciendo uso de las herramientas que para este fin 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 serán evaluados en un ambiente de pruebas para ser aprobados previo a su puesta a punto en producción.

Una vez que hayan sido probados los sistemas y todas las pruebas hayan sido satisfactorias, se generará la autorización vía comunicación oficial hacia el líder tecnológico para que este a su vez lleve a cabo la habilitación de las actualizaciones en el ambiente productivo para su puesta en marcha.

6.4Protección contra el código malicioso y descargable

6.4.1 Controles contra el código malicioso

Los equipos de cómputo de IMAGITECH 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

Todo el personal de IMAGITECH tiene prohibida la instalación, descarga o consulta de software en los equipos de cómputo, adicional al que se le proporciona para llevar a cabo sus funciones.

Como parte de las actividades de mantenimiento que se realizarán periódicamente a los equipos se incluirá la revisión de dichos aspectos y aquellos que se identifiquen podrán ser sometidos a lo descrito en el numeral 4.2.3 Proceso disciplinario de la presente política.

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 diario y los respaldos serán guardados por un periodo de mínimo 10 días. Los respaldos de información serán almacenados en medios seguros de nube. Los respaldos serán enfocados en la información de salud de las instancias creadas para los clientes de IMAGITECH.

6.6 Gestión de la seguridad de las redes

6.6.1 Controles de red

Debido a la naturaleza de nuestra operación y de los servicios que se proveen, en IMAGITECH no se implementará una red interna, únicamente se hará uso de una conexión a Internet, misma que será brindada por el proveedor de las instalaciones donde se llevan a cabo las operaciones de la empresa. Por lo anterior, IMAGITECH no implementará ningún control de seguridad adicional asociado con telecomunicaciones.

6.6.2 Seguridad de los servicios de red

Debido a la naturaleza de nuestra operación y de los servicios que se proveen, en IMAGITECH no se implementará una red interna, únicamente se hará uso de una conexión a Internet, misma que será brindada por el proveedor de las instalaciones donde se llevan a cabo las operaciones de la empresa. Por lo anterior, IMAGITECH no implementará ningún control de seguridad adicional asociado con telecomunicaciones.

Así mismo, el servicio de centro de datos contratado tendrás niveles de servicios que serán cumplidos por el proveedor respectivo, asegurando que en todo momento los clientes de IMAGITECH cuentan con acceso al sistema de información.

La conectividad de los clientes de IMAGITECH a internet, está fuera del alcance y es responsabilidad de ellos mismos poder contar una conexión estable para tener acceso al sistema de información.

6.7 Manipulación de los medios

6.7.1 Gestión de los medios extraíbles

El personal de IMAGITECH no estará autorizado para extraer 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 en el respositorio de nube corporativa. Las unidades extraíbles externas no se encuentran autorizadas y su uso collevará a una sanción correspondiente.

6.7.2 Retirada de medios

Este control no aplica ya que se prohibe el uso de medios extraíbles dentro de la empresa.

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. Para tal fin se habilitará un repositorio de información institucional con acceso únicamente a los empleados de la IMAGITECH autorizados.

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

6.7.4 Seguridad de la documentación del sistema

La documentación de los sistemas de información será tratada como información restringida, por lo que será almacenada digitalmente en el repositorio institucional con acceso controlado y sólo accesibles por personal autorizado.

6.8 Intercambio de información

6.8.1 Políticas y procedimientos de intercambio de información de salud

Todo intercambio de información que lleve a cabo el sistema IMAGITECH se apegará a la NOM-024-SSA3-2012, las guías de intercambio de información en salud publicadas por la Secretaría de Salud que establecen los formatos, catálogos y datos mínimos a intercambiar.

6.8.2 Acuerdos de intercambio

Todo intercambio de información se llevará a cabo con los datos especificados en las Guías de Intercambio de Información, haciendo uso de los catálogos indicados en aquellas que así se requiera o los que se indican en la NOM-024-SSA3-2012. De acuerdo con el numeral 6.8.1. del presente documento, dicho intercambio quedará sustentado en el cumplimiento de la normatividad asociada a los Sistemas de Información de Registro Electrónico para la Salud.

6.8.3 Medios físicos en tránsito

Si un medio donde exista información de salud debe abandonar las instalaciones, esto será notificado al Líder Ejecutivo o Líder Tecnológico para determinar la procedencia del movimiento y proveer medios de almacenamiento autorizados por la organización, mismos que sólo serán usados por el personal autorizado. Dicho tránsito será documentado de acuerdo con lo descrito en la política

6.8.4 Mensajería electrónica

Actualmente IMAGITECH 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

La Plataforma IMAGITECH únicamente llevará a cabo el intercambio de información con las Autoridades en Salud y a través de las guías de intercambio de información en salud establecidas por la DGIS, donde se establecen los mecanismos para llevar a cabo dicho intercambio de información en salud, motivo por el cual no se establece ningún control de seguridad adicional asociado a este rubro.

6.9 Servicios de comercio electrónico en salud

6.9.1 Comercio electrónico

Actualmente dentro de IMAGITECH 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 IMAGITECH 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 IMAGITECH 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

La Plataforma IMAGITECH cuenta con un registro de eventos y actividades donde cada vez que un usuario accede o sale del sistema, así como eventos relacionados con la prestación de servicios de salud del personal respectivo en cada una de las instancias de los clientes. Se almacenarán datos que identifiquen el usuario, tipo de perfil de usuario, equipo de cómputo, acción realizada, fecha y hora.

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 de este.

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 la Plataforma IMAGITECH.

6.10.5 Registro de fallos

Para los fallos ocurridos dentro de la operación de la Plataforma IMAGITECH, se mantendrá a través del sistema de CRM un registro y seguimiento de las incidencias detectadas por personal de IMAGITECH y reportadas por los usuarios del sistema.

6.10.6 Sincronización del reloj

La Plataforma IMAGITECH mantendrá una sincronización de reloj centralizada mediante un servidor NTP (Network Time Protocol) estándar y de acuerdo a la zona horaria donde operan sus clientes 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

La Plataforma IMAGITECH contará con un mecanismo de acceso que sólo permitirá la entrada al personal autorizado mediante usuario y contraseña. Dependiendo del rol y perfil, el sistema únicamente mostrará la información que le compete al usuario. El usuario administrador tendrá acceso a la lista de usuarios registrados.

7.2 Requisitos Gestión de acceso de usuario

7.2.1 Registro de usuarios

Los accesos al sistema de IMAGITECH mediante el cual se administra y procesa información de salud

estarán documentados en el listado de activos y serán autorizados por el grupo de seguridad de la información por medio de una carta de alta de usuarios emitida por los participantes del GSI.

7.2.2 Gestión de privilegios

De acuerdo con lo descrito en el numeral 6.1.3 Segregación de tareas, para cada una de las instancias que habilita IMAGITECH para sus clientes, se mantendrá actualizado un reporte de usuarios y las funciones que desempeña dentro de la plataforma IMAGITECH, con el fin de documentar que efectivamente cumplen con las funciones específicas que le competen al usuario.

7.2.3 Gestión de contraseñas de usuarios

En el manejo de contraseñas se debe tomar en cuenta:

- Contener mayúsculas y minúsculas
- Contener números
- Usar mínimo 8 caracteres
- No escribir la contraseña en un papel o documento donde quede constancia de ésta.
- No enviar nunca la contraseña por correo electrónico plano, considerar al menos archivos protegidos y canales seguros.
- No escribir las contraseñas en archivos sin protección o de los que se desconozca su nivel de seguridad.

Las contraseñas serán asignadas por el usuario con perfil de Administrador del Sistema y el usuario receptor de dichas credenciales será responsable de cambiar inmediatamente la contraseña temporal que se le haya asignado.

7.2.4 Revisión de los derechos de acceso de usuario

Dado que la organización permite a sus clientes el manejo autónomo de sus cuentas de usuario, el sistema les proveerán con las herramientas para poder administrar sus usuarios registrados. Para la administración de cada cuenta de usuario, el personal de IMAGITECH tendrá asignada una cuenta de usuario administrador, misma que será declarada en su listado de activos asignados.

7.3 Responsabilidades de usuario

7.3.1 Uso de contraseñas

Los usuarios de la Plataforma IMAGITECH tendrán 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 la Plataforma IMAGITECH 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 20 minutos, se deberán bloquear de forma automática y solicitar el inicio de sesión nuevamente.

7.3.3 Equipo Política de puesto de trabajo despejado y pantalla limpia

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

- No debe existir a la vista o a la mano documentos con información sensible o de salud.
- No debe haber dispositivos de almacenamiento externo
- Los escritorios y áreas de trabajo deberán estar libres de alimentos.
- El área de trabajo debe estar despejada, sólo con el material 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

Para poder tener acceso a los recursos de IMAGITECH que están disponibles únicamente mediante conexiones de red, los empleados autorizados utilizarán únicamente Secure Shell (SSH) para acceder a los recursos disponibles vía red.

7.4.2 Autenticación de usuario para conexiones externas

IMAGITECH no proporciona a externos acceso a sus recursos disponibles en red. Para el acceso a los servicios de red, los usuarios internos de IMAGITECH utilizan los mecanismos seguros de inicio de sesión.

7.4.3 Identificación de los equipos en las redes

IMAGITECH no cuenta con redes locales o intranet. Este control no es aplicable.

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

IMAGITECH no cuenta con redes locales o intranet. Este control no es aplicable.

7.4.5 Segregación de las redes

IMAGITECH no cuenta con redes locales o intranet. Este control no es aplicable.

7.4.6 Control de la conexión a la red

IMAGITECH no cuenta con redes locales o intranet. Este control no es aplicable.

7.4.7 Control de enrutamiento (routing) de red

IMAGITECH no cuenta con redes locales o intranet. Este control no es aplicable.

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 del personal de IMAGITECH estará protegido mediante un inicio seguro de sesión, complementado con la habilitación del pin adicional de BitLocker en aquellos equipos donde sea necesario.

7.5.2 Identificación y autenticación de usuario

Los nombres de usuario para las cuentas de acceso a la Plataforma IMAGITECH serán únicos para su uso personal y exclusivo, de tal forma que puedan ser identificados claramente. Dentro de la plataforma IMAGITECH será mostrado el nombre del usuario en todo momento para que se pueda confirmar que el usuario está trabajando en la sesión correcta.

7.5.3 Sistema de gestión de contraseñas

De acuerdo con los criterios establecidos para la gestión de contraseñas, en el alta de nuevos usuarios se deberán seguir lo descrito en el numeral 7.2.3 del presente documento. Dentro de la plataforma IMAGITECH se contará con un módulo para la administración de dichas contraseñas y que contará con las validaciones que permitan cumplir con los criterios establecidos.

7.5.4 Uso de los recursos del sistema

Dado que la plataforma IMAGITECH funciona en la nube, se garantizará que los recursos requeridos estén disponibles para asegurar su óptimo funcionamiento. Periódicamente se realizará un monitoreo del consumo y disponibilidad de recursos en el servidor.

Así mismo, en el servidor se tendrán instaladas únicamente las herramientas necesarias para el funcionamiento de la plataforma IMAGITECH.

7.5.5 Desconexión automática de sesión

Los equipos de cómputo de la empresa, después de veinte 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

Para el caso de la plataforma IMAGITECH, dadas las necesidades de la operación de los médicos que la utiliza, las sesiones se podrán mantener activas hasta por un periodo de 14 horas.

7.6 Control de acceso al sistema operativo

7.6.1 Restricción de acceso a la información

El acceso a la Plataforma IMAGITECH, respaldos del sistema, documentación, información compartida 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:

- Repositorios de información disponibles únicamente para usuarios autorizados
- Sistemas con accesos mediante nombre de usuario y contraseña.
- Documentación almacenada en espacios seguros 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 movidos únicamente bajo la autorización correspondiente del GSI según lo descrito en el numeral 5.2.5 Seguridad de los equipos fuera de las instalaciones.

7.7.2 Teletrabajo

Actualmente la Plataforma IMAGITECH 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 la Plataforma IMAGITECH, ésta se apegará a los siguientes controles de seguridad:

- Contará con un entorno dedicado para su ejecución en ambiente productivo.
- Los accesos a servidores web, de base de datos, 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

Dentro de la plataforma IMAGITECH en todo momento que se abra o inicie un expediente clínico de un paciente, se mostrará en todo momento en las pantallas del sistema el nombre de dicho paciente para que el personal médico los identifique.

Si un usuario es capturado dos veces la plataforma de IMAGITECH contará con un proceso para combinar y fusionar ambos expedientes clínicos.

8.2.2 Validación de los datos de entrada

La Plataforma IMAGITECH 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

La Plataforma IMAGITECH 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

En alineación con los controles 8.1.1 Análisis y especificación de los requisitos de seguridad y 8.2.1 Identificación única de sujetos de atención, la plataforma IMAGITECH mostrará en todo momento en pantalla los datos de identificación del paciente que está siendo sujeto de atención por el personal de salud. Se mostrarán datos generales de identificación como el nombre del paciente o en su defecto el identificador único 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 utilizarán serán únicamente en aquellos equipos de cómputo cuya unidad de almacenamiento sea cifrada a través de las herramientas autorizadas por el Líder Tecnológico. La administración de dichas herramientas estará a cargo del Líder Tecnológico y serán obligatorias para los empleados de IMAGITECH con equipos compatibles.

8.3.2 Gestión de claves

La gestión de las llaves a partir de las cuales se cifrarán los equipos de cómputo estará a cargo del personal responsable de dicho equipo, quien dentro de sus responsabilidades tendrá el resguardo seguro de dichas llaves en un repositorio seguro.

8.4 Seguridad de los archivos de sistema

8.4.1 Control del software en explotación

Actualmente dentro de IMAGITECH no existen sistemas que cuenten con módulos o software para la explotación de información, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

8.4.2 Protección de los datos de prueba del sistema

Queda prohibido el uso de información de salud de pacientes real en cualquier ambiente de pruebas o desarrollo. Se usarán datos ficticios creados para dichos fines.

8.4.3 Control de acceso al código fuente de los programas

El acceso al código fuente de la Plataforma IMAGITECH está restringido sólo al personal autorizado, así como el equipo de desarrollo de software. El código fuente será administrado a través de las herramientas de ingeniería y desarrollo de software que para este fin el Líder Tecnológico haya implementado.

8.5 Seguridad en los procesos de desarrollo y soporte

8.5.1 Procedimientos de control de cambios

Cualquier modificación que se realice a la plataforma IMAGITECH 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 seguir el siguiente procedimiento:

- El cliente o internamente IMAGITECH solicita llevar a cabo un cambio
- El líder ejecutivo o líder tecnológico aprueban la ejecución del cambio
- El equipo de desarrollo de software lleva a cabo el cambio
- Completado el cambio, el Líder Operativo llevará a cabo las pruebas
- Cuando las pruebas son exitosas se notifica al Líder Ejecutivo o Líder Tecnológico para que se autorice la liberación del cambio
- Se autoriza y liberan los cambios en ambiente productivo
- Se notifica a los clientes de IMAGITECH a través de Newsletters

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 Líder Tecnológico o Ejecutivo, las pruebas que se llevarán a cabo serán de todas las funciones para asegurar que el sistema trabaja correctamente. 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 será controlada a través del mecanismo que para este fin implemente el líder tecnológico, quien a su vez también controlará la liberación de nuevas versiones.

Todo cambio dentro de la Plataforma IMAGITECH debe estar plenamente justificado, y se deberá observar lo establecido en el numeral 8.5.1 Procedimientos de control de cambios.

8.5.4 Fugas de información

Para asegurarse que el software de la plataforma IMAGITECH no tenga fugas de información, el líder tecnológico implementará un mecanismo de control de acceso al mismo.

Respecto de las bases de datos de los clientes que utilizan la plataforma de IMAGITECH, únicamente se darán de alta los administradores de bases de datos y el usuario necesario para conectar la aplicación con la base de datos.

Aquella información que se determine sea posible exportar se pondrá a disposición de los usuarios a través de reportes programados en el sistema de IMAGITECH. Los reportes estarán disponibles de acuerdo con los roles y perfiles descritos en el numeral 6.1.3 Segregación de tareas.

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

Actualmente dentro de IMAGITECH se realizan todos los desarrollos de software, motivo por el cual no se establece ningún control de seguridad asociado a este rubro.

8.6 Gestión de las vulnerabilidades técnicas

8.6.1 Control de las vulnerabilidades técnicas

IMAGITECH buscará asegurarse que la Plataforma IMAGITECH 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 con los niveles 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

Todos los eventos de seguridad reportados por los usuarios de la plataforma serán registrados en el sistema de gestión de incidentes que para este fin tendrá habilitado IMAGITECH.

9.1.2 Notificación de puntos débiles de seguridad

Todo el personal interno y externo de IMAGITECH 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 los firmantes aceptarán la responsabilidad de notificar las observaciones o sospechas de puntos débiles a través del sistema de gestión de incidentes que para este fin tendrá

habilitado IMAGITECH.

9.2 Gestión de incidentes y mejoras de seguridad de la información

9.2.1 Responsabilidades y procedimientos

El Líder Operativo y el Líder Tecnológico serán responsables de monitorear la herramienta de gestión de incidentes.

Al detectar un incidente se realizará lo siguiente:

- Se notificará al líder tecnológico sobre el incidente.
- Se identificará en la base de conocimiento si existe un incidente similar en el pasado y se tratarán de aplicar las soluciones que hayan dado resultado anteriormente.
- El equipo técnico brindará la asistencia para resolver el incidente, determinando la magnitud del incidente.
    - Grave: Es una amenaza que pone en riesgo la continuidad operativa de la empresa
    - Media: Es un evento que tiene afectación parcial sobre la operación de la empresa y de no resolverse podría interrumpir la continuidad operativa
    - Baja: El impacto es mínimo o aún no se materializa, sin poner en riesgo la operación de la empresa, se deberá resolver con prontitud una vez que no haya ningún incidente de magnitud media o grave
- Dependiendo de la respuesta del equipo técnico se notificará vía la herramienta de gestión de incidentes a las partes involucradas para mantenerlas informadas sobre el estatus del incidente.
- Si el equipo técnico ha solucionado el incidente, se da por cerrado y se notifica a los involucrados.
- 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 de acuerdo con los procedimientos establecidos para dicho fin.
- Después se deberá verificar que se haya dado solución al incidente y se da por cerrado.

9.2.2 Aprendizaje de los incidentes

A partir de los incidentes de seguridad reportados, se documentará en una base de conocimiento el detalle de los incidentes y las acciones tomadas para resolver, a fin de buscar en ella posibles soluciones cuando se presenten incidencias en el futuro.

Se mantendrá un registro con los detalles del incidente e información asociada con las acciones que llevaron a una solución. La información estará disponible para consulta del líder tecnológico, líder operativo y líder ejecutivo, así como aquel personal adicional que apoye en la solución de incidentes.

9.2.3 Recopilación de evidencias

Todas las evidencias colectadas durante la atención y solución a los incidentes de seguridad deberán ser adjuntadas a los correos electrónicos que se emitan como parte de las comunicaciones en las diferentes etapas de la solución. Aquellos documentos anexos y complementarios que se hayan generado o transmitido durante la atención del incidente quedarán almacenadas en el repositorio seguro que para este fin será habilitado dentro de IMAGITECH.

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 en que la Plataforma IMAGITECH 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:

- Monitorear las operaciones diarias
- Identificación y registro de la falla
- Notificación al área responsable
- Aplicar las acciones correctivas
- Verificar el restablecimiento del servicio
- Monitorear el servicio posterior a la solución.

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 centro de datos
- Desastre natural
- Error crítico en la liberación de una nueva versión del sistema
- Ataques informáticos
- Error humano

En caso de que se identifique algún otro factor que ponga en riesgo la continuidad operativa de la plataforma IMAGITECH lo hará de conocimiento del GSI y demás usuarios involucrados.

10.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

Con el fin de guia, 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 IMAGITECH.

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 IMAGITECH, 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 la Plataforma IMAGITECH 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 para garantizar la continuidad del negocio.
- Establecer niveles de servicio con los terceros cuyos servicios prestados se relacionen con la continuidad operativa de la Plataforma IMAGITECH.

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 de la Plataforma IMAGITECH, IMAGITECH establece como el marco normativo, legal y jurídico aplicable las siguientes disposiciones:

- LFTAIP, Ley Federal de Transparencia y Acceso a la Información Pública.
- LFPDPPSO, Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados.
- NOM-024-SSA3-2012, Sistemas de Información para el Registro de Información en Salud

11.1.2 Derechos de propiedad intelectual (IPR)

En cumplimiento y garantía de la propiedad intelectual de la Plataforma IMAGITECH y demás activos de información relacionados, IMAGITECH contará con la documentación que acredite ante las

autoridades correspondientes la titularidad o propiedad del sistema.

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. Estos medios garantizarán la protección contra la pérdida o extracción no autorizada de la información. Los medios para resguardo podrán incluir cajas fuertes o repositorios digitales de información con controles de acceso.

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 sitio web de IMAGITECH se encontrará disponible para consulta:

- ☐ Términos y condiciones de uso
- ☐ Política de uso de cookies
- ☐ Aviso de privacidad.

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 y su sitio web, IMAGITECH llevará a cabo la difusión correspondiente a través de diversos medios, tales como correo electrónico y aquellos que la organización determine para disuadir a los usuarios y personal en general del uso de la información para fines no autorizados.

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 este 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 asegurarán 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 la Plataforma IMAGITECH 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 SGSI.

El Líder Ejecutivo estará al tanto de las nuevas publicaciones que haga la autoridad en salud para determinar la aplicabilidad de nuevas regulaciones o actualización de las existentes.

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 la Plataforma IMAGITECH, 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.Se realizarán revisiones trimestrales

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.