P

Políticas

POLÍTICA

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN"

VERSIÓN 1.0

MAYO 2018

TABLA DE CONTENIDOS

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

1. DECLARACIÓN

Rayen Salud reconoce que la información es un bien estratégico que, como otros bienes de la organización, tiene gran valor y necesita ser protegida tanto en su integridad, confidencialidad y disponibilidad. La seguridad de la información protege una gran gama de amenazas con el fin de asegurar la continuidad de las operaciones, minimizar el daño y maximizar la eficiencia y las oportunidades de mejora.

Cualquier forma que tome la información, ya sea documentos en papel, documentos digitales, base de datos, sistemas y software de aplicación, personas, equipos informáticos, redes de transmisión de datos, enlaces de terceros, datacenter, soportes de almacenamientos y otros elementos de infraestructura, siempre debe estar protegida en forma adecuada.

Para Rayen Salud, es de alta importancia la protección de la información y de sus procesos, representados en gran parte por la infraestructura tecnológica de información y comunicaciones (TIC). Por lo tanto, todo el personal de Rayen Salud, será responsable de la confidencialidad, integridad y disponibilidad de la información, que, por cargo y función, le corresponde.

2. OBJETIVO GENERAL

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información relevante, con el objeto de asegurar la continuidad operacional del negocio, a través de un Sistema de Gestión de Seguridad de la Información.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

3. ALCANCE

La presente Política de Seguridad de la Información expresa, en forma clara los lineamientos generales, respecto al buen uso de los Activos de información, tanto compartidos como de cada uno de los usuarios internos o externos. Fija las directrices y soporte para la seguridad de la información en concordancia con los requerimientos de la empresa, leyes y regulaciones pertinentes.

Estos lineamientos, están destinados a servir de guía para la definición de normas específicas, que serán parte de las disposiciones complementarias de carácter administrativo y técnico que se dicten para el cumplimiento de lo dispuesto en la presente Política.

La Seguridad de la Información es responsabilidad de todos los usuarios que se relacionan con la empresa, ya sean usuarios externos identificables que presten servicios o asesorías y que por sus funciones deban acceder a las instalaciones de Rayen Salud, o usuarios internos con acceso a los Activos de Información. Por tal razón, las políticas establecidas en este documento son de conocimiento y cumplimiento obligatorio tanto para internos como externos, cuya obligación deberá expresarse en los contratos y/o acuerdos respectivos.

4. CONTROL Y SANCIONES

El incumplimiento de lo definido en esta política será considerado falta, y podrá ser sancionado de acuerdo con la gravedad de ésta, previa evaluación de la intencionalidad, impacto y daño que cause en Rayen Salud, según lo indicado en proceso de Sanción Disciplinaria.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

5. DOCUMENTOS DE REFERENCIA

- Norma ISO 27001:2013, clausula 5.2
- Controles: A 5.1.1

6. GLOSARIO DE TÉRMINOS

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

a. Activo: Cualquier elemento que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:
   - Activos de Información: se entenderá por Activo de Información todo elemento en que se registre, se almacene y/o procese datos e información, sea a través de medios tecnológicos o no, tales como: personas, bases de datos y archivos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, plan de continuidad de negocio, información de auditorías, información archivada, activos de software, activos físicos y servicios.
   - Activos de Software: constituidos por las aplicaciones de software, Software de sistemas y Herramientas de desarrollo y utilidades.
   - Activos Físicos: constituidos por el equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.

b. Servicios: servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)

c. Personas: constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.

d. Intangibles: constituidos por los activos referidos a la reputación e imagen de la empresa.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

e. Amenaza: una causa potencial de un incidente no-deseado, el cual puede derivar en daño a un sistema u organización.

f. Análisis de Riesgos: uso sistemático de la información para identificar las fuentes y calcular el riesgo.

g. Confidencialidad: garantía de que accedan a la información sólo aquellas personas autorizadas a hacerlo.

h. Integridad: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.

i. Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

j. Política: intención y dirección general expresada formalmente por la autoridad máxima en la institución.

k. Riesgo: combinación de la probabilidad de un evento y su ocurrencia.

l. Seguridad de la Información: preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

m. Sistema Informático: constituido por el conjunto de computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

n. Software malicioso: también conocido como Malware (del inglés "malicious software") entendiéndose por tal todo software que tiene como objetivo infiltrarse en un sistema informático y dañar la (o las) computadora(s) que lo sustenta(n) sin el conocimiento de su dueño, con finalidades muy diversas. En esta categoría, encontramos desde Virus informáticos hasta Troyanos y Spyware.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

o. El Malware hace referencia a una variedad de software o programas de códigos hostiles e intrusivos. Se debe considerar que el ataque a la vulnerabilidad por malware puede ser a una aplicación, una computadora, un sistema operativo o una red completa.

p. Tecnología de la Información y de las Comunicaciones (TIC): constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: LIDERAZGO Y COMPROMISO

Considerando que:

- La Alta Dirección debe procurar una correcta administración de la información de la organización y velar por su adecuado uso, conservación y mantenimiento, conforme a leyes, normas y acuerdos contractuales;
- La empresa debe resguardar los activos de información que son de su propiedad para asegurar la confidencialidad, integridad y disponibilidad de estos;

Procede a definir, establecer, aprobar, implementar, publicar, comunicar, revisar, monitorear, manejar y mejorar continuamente la Política de Seguridad de la Información, lo cual permita prevenir, detectar y corregir cualquier amenaza y/o vulnerabilidad asociada a la información de la organización.

Por ello, Rayen Salud reconoce que la seguridad de la información tiene alta prioridad para cumplir la misión de sus compromisos legales, normativos y

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

contractuales, lo que constituye un alto compromiso de la Alta Dirección y de la totalidad de sus colaboradores.

Los criterios y lineamientos relacionados con la Seguridad de la Información de la empresa se establecen mediante un marco normativo, con políticas y procedimientos que faciliten disponer de estándares para manejar, generar, procesar, intercambiar y almacenar los activos de información, de manera de obtener los niveles de Confidencialidad, Integridad y Disponibilidad que permitan la continuidad de las operaciones.

Para cumplir con lo señalado, se ha establecido el siguiente Compromiso de la Dirección:

La Alta Dirección provee evidencia de su compromiso con el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información –SGSI– conforme a ISO/IEC 27001:2013, así como la mejora continua de su efectividad mediante las siguientes acciones:

a. Autorizando la implementación y aprobación del SGSI.
b. Estableciendo la política y objetivos del SGSI.
c. Asignando roles y responsabilidades en seguridad de la información.
d. Asegurando que la Política de Seguridad de la Información es comunicada, conocida y entendida por todos y cada uno de los colaboradores que pertenecen a la organización, así como también por sus proveedores, clientes y terceras partes.
e. Proporcionando los recursos necesarios para la correcta implementación del SGSI.
f. Asegurando que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

g. Mejorando continuamente los procesos, mediante el Sistema de Gestión de la Seguridad de la Información, conforme a las directrices establecidas en la Norma Internacional ISO 27001:2013.

h. Satisfaciendo los requerimientos de sus clientes en temas de seguridad de la información, asignando los recursos necesarios para lograr un óptimo desempeño.

i. Promoviendo la seguridad de la información, comprometiendo para ello la participación de todo su personal, valorando su participación y aportes.

j. Promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información, para aumentar la competitividad en el mercado, utilizando herramientas de control de procesos, auditorías, análisis de riesgos, capacitaciones y concienciación de todos los actores involucrados para comprometer su participación.

k. Asegurando la actividad constante de la organización, en función de los requerimientos legales, reglamentarios y contractuales de seguridad de la información.

l. Manteniendo a través del tiempo la fortaleza de la tríada fundamental de la seguridad de la información, esto es, Confidencialidad, Integridad y Disponibilidad.

m. Revisando la Política de Seguridad de la Información a intervalos planificados de 1 año, coincidiendo con la realización de la Revisión del SGSI por la Dirección y/o cuando se produzcan cambios significativos, con el fin que se mantenga idoneidad y adecuación, asegurando así su conveniencia, suficiencia y eficacia continua, dejando registro de estas revisiones.

n. Apoyando la definición y establecimiento de políticas, procedimientos, instructivos y planes asociados a seguridad de la información que sean necesarios en la organización.

www.rayensalud.com
-56 2 2588 8800
Mercced 480 - Piso 2, Santiago
Región Metropolitana

La revisión de la presente Política de Seguridad de la Información incluye las oportunidades de mejora, como respuesta a los cambios que pudiesen aparecer, como son aquellos normativos, legales, contractuales, tecnológicos, operacionales, administrativos, organizacionales, impactos de eventos e incidentes de seguridad, cambios no planeados, cambio en los costos de los controles aplicados, entre otros factores. Aquellas mejoras identificadas deben quedar registradas y ser aprobadas por quienes se identifican como responsables del manejo de la presente Política.

La definición de la política del SGSI para los procesos establecidos incluye los siguientes tópicos:

7.1 Organización de la Seguridad de la Información

El objetivo es establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la Seguridad de la Información dentro de la organización.

Para ello, busca establecer un modelo de gerenciamiento para:

a. Controlar la implementación del sistema y la definición clara de funciones y responsabilidades.
b. Elaborar políticas con conformidad a las directrices establecidas en la Norma ISO/IEC 27001:2013 y que sean adecuadas a los requerimientos de Seguridad de la Información aplicable al alcance del SGSI.
c. Definir y establecer mecanismos de actualización periódica de las políticas, procedimientos y/o instructivos.
d. Mejorar la seguridad de la información en los procesos establecidos en el alcance del SGSI.
e. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceras partes a la información.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

Con ese objetivo se crea el Comité de Seguridad de la Información, el que estará presidido por el Oficial de Seguridad de la Información (OSI) - cuyas funciones y responsabilidades están definidas y establecidas en el documento descripción de cargos - y conformado por quienes designe la alta dirección de la empresa, lo que será consignado debidamente en un acta de constitución de dicho Comité.

La misión y acciones de dicho comité estarán detalladas en el documento de descripción de cargo correspondiente. Este comité sesionará las veces que sea necesario conforme a los requerimientos de seguridad que se sucedan.

La función fundamental del Comité de Seguridad es asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información establecidos en el alcance del SGSI, así como los medios que soporten la información, sean estos tecnológicos o de otro tipo. Para ello elaborará políticas, procedimientos e instructivos, manteniéndolos vigentes en mejora continua.

Se debe tener en cuenta que determinadas actividades pueden requerir el acceso de terceros a la información interna, así mismo, externalizar hacia terceros algunas funciones relacionadas con la información que se maneja dentro del alcance del SGSI. En caso de que ello suceda, se tendrá en consideración que la información puede estar expuesta a riesgos si las terceras partes acceden en el contexto de una administración deficiente en relación a la gestión de la seguridad de la información, motivo por el cual serán establecidas las medidas apropiadas para protegerla.

Este aspecto de la Política se aplica a todos los recursos del área establecida en el alcance y a todas sus relaciones con terceras partes que requieran tener acceso a los activos de información establecidos dentro del alcance del SGSI.

7.1.1 Contacto con Autoridades

Dentro del alcance del SGSI, se mantienen los contactos apropiados con las autoridades pertinentes al cumplimiento de la ley, entidades

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

regulatorias, autoridades de supervisión, proveedores de servicios básicos y telecomunicaciones, servicios de emergencia, electricidad, agua, salud, seguridad, bomberos, entre otras, cuando corresponda, en caso de existir un evento o incidente de seguridad, informando los incidentes de seguridad de la información identificados de manera oportuna, conforme a los lineamientos establecidos en el procedimiento Gestión de Incidentes de Seguridad. Se utiliza para ello un documento interno con la lista de contactos y un breve instructivo de cómo proceder.

7.1.2 Contacto con Grupos de Interés Especial

Dentro del alcance del SGSI, se mantienen los contactos adecuados con grupos de interés especiales y/o foros especializados en seguridad, así como asociaciones de profesionales. Ello, para apoyar el mejoramiento del conocimiento sobre las buenas prácticas y permanecer al tanto de la información de seguridad pertinente; asegurarse de que la comprensión del entorno de seguridad de la información sea actual y completo; recibir información temprana de avisos, parches y alertas en general, relacionados con ataques y vulnerabilidades; obtener acceso a información de especialistas sobre consejos de seguridad; compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas y vulnerabilidades; proporcionar puntos de enlace adecuados al tratar con incidentes de seguridad de la información. Los contactos que conforman los grupos de interés especial, foros de seguridad de especialistas y asociaciones profesionales se enumeran en un documento interno con las instrucciones pertinentes.

7.1.3 Seguridad de la Información en la Gestión de Proyectos

Dentro del alcance del SGSI, sin importar el tipo de proyecto, se integra la Seguridad de la Información en los métodos de administración de proyectos, para asegurarse de que se identifican y abordan los riesgos de

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

seguridad de la información como parte de un proyecto, sin importar su carácter. Para ello, los métodos de administración de proyectos deben incluir los objetivos de seguridad de la información en los objetivos del proyecto; realizar una evaluación de riesgos de seguridad de la información antes de iniciar el proyecto de manera de definir y establecer los controles que sean necesarios, estableciendo que la seguridad de la información sea parte de todas las fases de la metodología aplicada al proyecto.

7.2 Seguridad de Recursos Humanos

Su objetivo es:

a. Asegurar que los colaboradores y contratistas entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.
b. Asegurar que los colaboradores y contratistas estén en conocimiento y cumplan con sus responsabilidades de Seguridad de la Información.
c. Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.
d. Reducir los riesgos en el manejo de información y establecer compromisos y mecanismos necesarios para fortalecer las debilidades en materia de seguridad a este respecto.
e. Considerar en los procesos de selección, incorporación, capacitación y desvinculación de Gestión de Personas, aquellos roles necesarios que permitan mantener el debido resguardo de los activos de información.
f. Para resguardar los activos de información en relación a Gestión de Personas, se realizarán las siguientes acciones, no siendo la siguiente lista taxativa:
    - Definir roles, cargos y accesos del personal perteneciente a la empresa a los activos de información definidos y establecidos dentro del alcance del SGSI.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

- Incluir en forma permanente en el proceso de reclutamiento de personal, las políticas, procedimientos e instructivos establecidos por la empresa.
- Establecer durante los procesos de capacitación, inducción, charlas, talleres y formación en general, los deberes y responsabilidades, correspondientes al personal y a la empresa en general, en materia de Seguridad de la Información.
- Capacitar al personal en aquellas materias relacionadas a Seguridad de la Información.
- Definir, establecer, implementar, controlar, mantener y mejorar políticas y/o procedimientos de resguardo de activos de información en los procesos de desvinculación del personal.

7.3 Gestión de Activos

Su objetivo es:

Identificar y mantener la debida protección de los activos de información establecidos en el alcance del SGSI, realizando para ello las siguientes actividades:

a. Clasificar y elaborar un inventario de los activos de información de la empresa.
b. Realizar la identificación, análisis, evaluación y tratamiento de riesgos que pudiesen estar presentes para los activos de información.
c. Identificar y clasificar aquellos activos de información que forman parte de los procesos estratégicos de la empresa, de manera que asegure la continuidad de las operaciones y del negocio.
d. Mantener actualizado el inventario de los activos de información, conforme a su tipo, formato, ubicación física y/o virtual según corresponda, importancia, responsable y procedimiento de manipulación, proveyendo adicional protección a aquellos activos de información que lo requieran dentro del marco legal.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

e. Efectuar análisis de los riesgos asociados a los activos de información, de acuerdo a su importancia y ubicación, de manera de determinar, en forma permanente, las posibles brechas de seguridad existentes para determinar las mejores medidas de mitigación que permitan minimizar los riesgos que pudiesen amenazar la continuidad de las operaciones y del negocio.
f. Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.

7.4 Control de Acceso

Su objetivo es:

a. Restringir el acceso a la información y a las instalaciones de procesamiento de la información.
b. Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.
c. Responsabilizar a los usuarios del cuidado de su información de autenticación.
d. Evitar el acceso sin autorización a los sistemas y aplicaciones.
e. Validar, verificar y proveer el acceso lógico a la información (aplicaciones, bases de datos y servicios en general) de forma adecuada.

Cada usuario de los activos de información tendrá acceso a los datos de las aplicaciones informáticas definidas en el alcance del SGSI, de acuerdo al rol que tenga definido su cargo y al nivel de acceso que le haya asignado la Jefatura Directa. Estos privilegios de acceso entregados a usuarios internos y externos estarán basados en la necesidad de uso, con el mínimo de información de acuerdo a su rol y funciones definidos dentro del alcance del SGSI.

La información a la que tengan acceso el personal es de exclusivo uso para desarrollar sus tareas conforme al alcance definido para el SGSI, de acuerdo a su rol y tareas asignadas, no pudiendo ser entregada ni divulgada de ninguna

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

forma, ni integral ni parcial a terceras partes que no sean sus superiores inmediatos y dentro del contexto del trabajo encomendado.

Se podrá acceder a la información de acuerdo a un plan de cuentas de acceso usuario, diseñado y controlado por la Gerencia Corporativa de Operaciones contenido en el alcance del SGSI, aprobado por el Comité de Seguridad de la Información de la empresa.

No se requiere contar con procedimientos de Inicio de Sesión Segura (Control 9.4.2 de la norma), dado a que es requisito suficiente el cumplimiento con la Política de Control de Acceso y con que los sistemas de información cuentan con un sistema de login, que contemple usuario y contraseña.

7.5 Criptografía

Su objetivo es:

Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información. Para ello será desarrollada una política sobre el Uso de Controles Criptográficos.

7.6 Seguridad Física y del Entorno

Su objetivo es:

a. Evitar accesos físicos no autorizados, interferencias contra las instalaciones de procesamiento de la información y la información de la organización contenida en el alcance del SGSI.
b. Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la empresa contenidas en el alcance del SGSI.

Serán consideradas áreas de acceso restringido, las instalaciones en las que se encuentren equipos de procesamiento o comunicaciones de datos, conforme al

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

alcance del SGSI, como son sala de servidores, dependencias donde se encuentran equipos de comunicaciones pertenecientes al cableado estructurado de la red, oficina de administradores y monitoreo, soporte, estaciones de trabajo y las instalaciones que el Comité de Seguridad de la Información determine deban ser de acceso restringido.

7.7 Seguridad de las Operaciones

Su objetivo es:

a. Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.
b. Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.
c. Proteger en contra de la pérdida de datos.
d. Registrar eventos y generar evidencia.
e. Asegurar la integridad de los sistemas operacionales.
f. Evitar la explotación de las vulnerabilidades técnicas.
g. Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

7.8 Seguridad de las Comunicaciones

Su objetivo es:

a. Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo, dirigido a mantener disponible y en correcto funcionamiento las instalaciones definidas en el alcance del SGSI.
b. Mantener la Seguridad de la Información transferida dentro del alcance del SGSI y con cualquier entidad externa.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

La Gerencia Corporativa de Operaciones gestionará el apoyo, servicios informáticos y de Seguridad de la Información, a las áreas definidas en el alcance SGSI, de acuerdo a lo establecido por el Comité de Seguridad de la Información de la empresa.

A su vez, el Comité de Seguridad de la Información definirá los procedimientos a seguir en la Gestión de Incidentes de Seguridad, que serán implementados por las áreas contenidas en el alcance del SGSI, con la coordinación del Oficial de Seguridad de la Información.

Se llevarán a cabo auditorías internas, conforme a necesidades establecidas por las Jefaturas del área, sin perjuicio de auditorías internas planificadas por la empresa.

Se deberá implementar mecanismos de protección preventiva y activa contra software maliciosos, que pudiesen penetrar en forma física y/o lógica a la red o estaciones de trabajo.

La información de los sistemas y configuraciones de los servidores de servicios importantes para las funciones del área contenida en el alcance del SGSI, se deberán respaldar periódicamente por esta área, conforme a lo definido por el Comité de Seguridad de la Información.

Para asegurar un adecuado uso de los servicios informáticos por parte de los usuarios internos o externos del área definida en el alcance del SGSI, ésta propondrá normas de uso de los servicios que estén a disposición del personal o de otras instituciones que hacen uso de los Activos de la Información contenidos en el alcance del SGSI, las que deberán ser aprobadas por el Comité de Seguridad de la Información.

7.9 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Su objetivo es:

www.rayensalud.com
+56 2 2588 8800
Mercced 480 - Piso 2, Santiago
Región Metropolitana

a. Asegurar que la Seguridad de la Información es parte integral de los sistemas de información en todo el ciclo.
b. Asegurar que la Seguridad de la Información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.
c. Asegurar la protección de los datos usados para prueba.

Todo Activo de Información necesario de incorporar en el área contenida en el alcance del SGSI, será evaluado por el Comité de Seguridad conforme a un análisis de riesgos, de manera de considerar antes de la compra, los requerimientos de seguridad que correspondan a tales activos de información.

Todo software operacional debe ser controlado, administrado y mantenido en una biblioteca técnica, junto a todas sus actualizaciones.

Software computacional, compilaciones de datos, adaptaciones y cualquier documento relacionado con ello, son propiedad de la empresa, en caso de aquellos realizados por personal de la empresa, en el desempeño de sus funciones, ya sea porque éstos se construyesen en forma individual o colectivamente.

Los Activos de Información identificados como importantes para la continuidad de las operaciones y del negocio en el alcance del SGSI, deben contar con contrato de mantenimiento y/o soporte con los proveedores que correspondan, de manera de asegurar su funcionamiento o reemplazo de acuerdo a niveles de servicio requeridos y su actualización.

7.10 Relación con Proveedores

Su objetivo es:

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

a. Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.
b. Mantener un nivel acordado de Seguridad de la Información y entrega del servicio, en línea con los acuerdos del proveedor.

7.11 Gestión de Incidentes de Seguridad de la Información

Su objetivo es:

Asegurar un enfoque consistente y eficaz sobre la Gestión de los Incidentes de Seguridad de la Información, incluida la comunicación sobre eventos de seguridad y debilidades.

7.12 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del negocio

Su objetivo es:

a. Incorporar la Continuidad de la Seguridad de la Información en los Sistemas de Gestión de Continuidad de Negocio de la organización.
b. Asegurar la disponibilidad de las instalaciones de procesamiento de la información.
c. Minimizar el impacto causado por interrupciones en las actividades ejecutadas dentro del alcance del SGSI, protegiendo los procesos críticos de eventos significativos funestos que pudieran presentarse.

Se establece una estrategia, aprobada por el Comité de Seguridad de la Información, que asegure continuidad de las operaciones y del negocio contenidos en el alcance del SGSI, considerados como procesos críticos. Así mismo, deberá gestionar los planes de contingencia, conforme a la estrategia definida.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

El Oficial de Seguridad de la Información, asumirá la responsabilidad de ejecución de la planificación de contingencia que permita asegurar la continuidad de los procesos críticos.

7.13 Cumplimiento

Su objetivo es:

a. Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la Seguridad de la Información y todos los requisitos de seguridad.
b. Asegurar que la Seguridad de la Información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.
c. Impedir posibles infracciones o violaciones a las normas, reglamentos, contratos y requisitos de Seguridad de la Información que se establezcan como parte de la implementación definida para el alcance del SGSI.

Cualquier transgresión de cualquiera de los puntos establecidos en la presente Política de Seguridad de la Información de Rayen Salud, dará lugar a la aplicación de sanciones disciplinarias.

8. Roles y Responsabilidades

De acuerdo con las responsabilidades, se decide quién está autorizado a acceder a qué tipo de información.

Estos se encuentran definidos, establecidos, documentados y detallados en el documento Roles y Responsabilidades del SGSI.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana

9. DIFUSIÓN

a. Todo el Personal de Rayen Salud deberá tomar conocimiento de la presente política.

b. Esta quedará disponible para consultas en la plataforma documental del Sistema de Gestión de Seguridad de la Información.

10. REGISTROS

No Aplica.

www.rayensalud.com
-56 2 2588 8800
Merced 480 - Piso 2, Santiago
Región Metropolitana