# POLÍTICA

# DE SEGURIDAD DE LA INFORMACIÓN (SI)

# POLÍTICA
# DE SEGURIDAD DE LA INFORMACIÓN (SI)

## INTRODUCCIÓN

La SUPERINTENDENCIA DE SERVICIOS DE SALUD (en adelante SSSalud) reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, la modificación y la utilización no autorizada de toda información relacionada con activos, clientes, empleados, haberes, códigos fuente, procesos internos, estrategia, gestión y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

La seguridad de la información se caracteriza como la preservación de:

a) su confidencialidad, de modo que sólo quienes estén autorizados puedan acceder a la información;

b) su integridad, de modo que la información y sus métodos de proceso sean exactos y completos;

c) su disponibilidad, de modo que solo los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.

La información se considera un activo de la SSSalud, la cual se expone a riesgos y amenazas de manera dinámica, que pueden provenir desde dentro o fuera de la misma y pueden ser intencionales o accidentales. Su ocurrencia puede provocar pérdidas materiales y económicas, daños en la imagen institucional y en la confianza de los ciudadanos, infracciones legales, incumplimiento regulatorio, vulnerabilidad de derechos, etc.. La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como normas, prácticas, procedimientos, estructuras organizativas y funciones de software.

Sobre la base de lo expuesto, es importante proteger adecuadamente los activos de información de la organización. Por ello, para la SSSalud la Seguridad de la Información es un proceso continuo destinado a proteger sus activos de información frente a las amenazas que pongan en riesgo la confidencialidad, integridad, disponibilidad de sus datos.

Toda información de la organización, independiente de la forma en que se documente (soporte), debe ser protegida adecuadamente a través de la implementación de un conjunto de controles, que se definen como normas y procedimientos de Seguridad de la Información.

## 1. OBJETIVOS

Esta Política de Seguridad de la Información tiene como objetivos:

- Establecer las directrices y criterios sobre el Sistema de Gestión de Seguridad de la Información SGSI, aplicables en la SSSalud, en los cuales se basan las normas y procedimientos.
- Orientar las acciones vinculadas al Sistema de Gestión de Seguridad de la Información que lleve adelante y comprometer a todas las áreas de la SSSalud, para que estén alineadas con los objetivos del servicio.

## 2. ALCANCE

Esta Política de Seguridad de la Información aplica a todos los activos de información de SSSalud; entendiendo como activos a los recursos de los sistemas de información o elementos relacionados con los mismos, necesarios para que la organización funcione correctamente y alcance los objetivos misionales. Asimismo, los recursos de Tecnología de Información (TI) comprenden procesos, datos, aplicaciones, tecnología, instalaciones y personal.

Por lo tanto, es responsabilidad de todos los funcionarios y agentes de SSSalud, además, de los destinatarios y los proveedores, cuando corresponda, conocer, cumplir y hacer cumplir cabalmente las disposiciones de esta Política SI.

## 3. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

Se establecen y se consideran como parte de este marco normativo de Seguridad de la Información, las Directrices establecidas en los Requisitos Mínimos de Seguridad de la Información, en un todo de acuerdo con la DA 641/2021:

1. **Política de Seguridad de la Información del organismo**.

   Esta Política SI debe estar basada en una evaluación de los riesgos que pudieran afectar a la SSSalud y debe ser:
   - notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.
   - cumplida por todos los agentes y funcionarios del organismo.
   - revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.
   - utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en SSSalud, su plataforma tecnológica y demás recursos de los que disponga.

   Áreas responsables de la implementación: USI - GG - CGG - Comité SI – SRHYO

2. **Aspectos organizativos de la seguridad.**

   Desarrollo e implementación de un marco organizativo que habilita una efectiva gestión y operación de la seguridad de la información en la SSSalud.
   Para tal fin se debe:
   - asignar a un área del organismo, con competencia en la materia,
   - delimitar las responsabilidades relativas a la seguridad de la información, y
   - segregar las funciones y áreas de responsabilidad.

Áreas responsables de la implementación: USI - GG - CGG - GAJ - GA – GSI

**3. Seguridad Informática de los Recursos Humanos.**

Adoptar una perspectiva sistémica para proteger los activos de información, considerando al personal como un recurso central. Establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad. Concientizar y capacitar a los agentes y funcionarios para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos.
Para tal fin se debe:

- realizar e implementar planes de concientización en el uso seguro y responsable de los activos de información,
- promover el entrenamiento permanente,
- establecer la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información,
- incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral,
- requerir a los agentes y funcionarios, cuando el Organismo lo considere necesario, de acuerdo a sus competencias, la firma de un acuerdo de confidencialidad, e
- incorporar dentro de los procesos disciplinarios cualquier violación a las Política SI del Organismo.

Áreas responsables de la implementación: CGG - SRHYO - GSI

**4. Gestión de activos.**

Gestionar y proteger en forma efectiva los activos de información del Organismo.
Clasificar según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, teniendo en cuenta sus funciones, la normativa que les sea aplicable y cualquier otro activo que pudieran contener de otros organismos públicos o entidades privadas, permitiendo adoptar las medidas de protección adecuadas.
Para tal fin se debe:

- clasificar los activos de información de todo el Organismo,
- llevar un inventario actualizado de todos los activos de información,
- gestionar la recepción y devolución de los activos de información, y
- efectuar una destrucción segura de cualquier medio que pueda contener información o datos personales.

Áreas responsables de la implementación: CGG - SRHYO - GSI - GA – PROPIETARIO

**5. Autenticación, Autorización y Control de Accesos.**

Definir e implementar procesos y mecanismos de seguridad según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. Los privilegios de

acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones.
Para tal fin se debe:

- gestionar, en forma adecuada y oportuna, las altas y bajas de cuentas de usuario y privilegios.
- establecer, para los agentes, funcionarios y demás usuarios, un uso responsable de sus dispositivos y datos de autenticación.
- realizar un seguimiento detallado sobre las cuentas con privilegios especiales.
- revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.

Áreas responsables de la implementación: CGG - SRHYO - GSI

**6. Uso de herramientas criptográficas.**

Proteger la confidencialidad, integridad, autenticidad y/o no repudio de la información del Organismo, mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.
Para tal fin se debe:

- cifrar cualquier dispositivo del Organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.
- proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.
- utilizar certificados digitales en todos los sitios de Internet del Organismo.

Áreas responsables de la implementación: CGG - GSI

**7. Seguridad física y ambiental**.

Proteger los activos de información del Organismo mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.
Para tal fin se debe:

- Identificar y proteger las áreas seguras contra desastres naturales, ataques maliciosos o accidentales.
- Incorporar controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.
- registrar los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.
- Adoptar medidas de seguridad para que el equipamiento sea ingresado o retirado del Organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.

- proteger los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.
- adoptar medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del Organismo y la interrupción de sus operaciones.
- incorporar medidas de protección que impidan interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.
- realizar un adecuado mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continuas.
- adoptar medidas de seguridad para los activos informáticos que deben llevarse fuera del Organismo.

Áreas responsables de la implementación: SRHYO - GSI - GA - RSF

**8. Seguridad operativa.**

Desarrollar, en forma segura, las operaciones del Organismo, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para tal fin se debe:

- establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.
- revisar, monitorear y ajustar los requerimientos de capacidad.
- minimizar los riesgos de acceso o de cambios no autorizados en entornos productivos.
- implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del Organismo.
- proteger las instalaciones contra infecciones de código malicioso.
- realizar copias de resguardo del software y la información, probándolas periódicamente.
- llevar registro de todos los eventos de seguridad y revisarlo periódicamente.
- mantener un control estricto sobre el software y su integridad, en entornos productivos.
- identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado.
- gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.
- registrar y revisar periódicamente las actividades de los administradores y operadores.

Áreas responsables de la implementación: CGG - GSI

**9. Seguridad en las comunicaciones**.

Proteger y controlar adecuadamente la información de las redes del Organismo, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del Organismo.

Para tal fin se debe:

- segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.
- proteger adecuadamente la información que se transfiera dentro del Organismo y hacia cualquier entidad externa.
- exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del Organismo.
- incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del Organismo en todos los acuerdos que se suscriban.

Áreas responsables de la implementación: CGG - SRHYO - GSI - GAJ – GA

**10. Adquisición, desarrollo y mantenimiento de sistemas de información.**

Contemplar la seguridad de la información como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet.

Para tal fin se debe:

- especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño).
- utilizar una metodología de desarrollo seguro.
- controlar los cambios que se realicen a las aplicaciones.
- proteger los datos utilizados en las pruebas.
- utilizar protocolos que garanticen la transmisión o enrutamiento adecuados.
- evaluar la seguridad de las aplicaciones antes de ponerlas productivas.
- proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.

Áreas responsables de la implementación: GSI

**11. Relación con proveedores.**

Incluir, en el pliego de bases y condiciones particulares en la contratación, cualquiera sea la modalidad, realizada por el Organismo para la provisión de un bien o servicio, cláusulas de cumplimiento efectivo por parte del contratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

Para tal fin se debe:

- considerar aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.
- establecer e incluir, en el pliego de bases y condiciones particulares, todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar,

almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al Organismo.
- supervisar, por parte de los responsables asignados al proyecto, todos los niveles de seguridad acordados.
- incluir cláusulas para mantenimiento del nivel de servicio.

Áreas responsables de la implementación: CGG - GA - GAJ - UR

**12. Gestión de incidentes de seguridad.**

Adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

Para tal fin se debe:
- llevar a cabo estudios de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.
- establecer e incluir en los pliegos de bases y condiciones particulares los requisitos de seguridad de la información pertinentes.
- supervisar y revisar, por parte de los responsables asignados al proyecto, todos los niveles de seguridad acordados.
- incluir cláusulas para mantenimiento del nivel de servicio.

Áreas responsables de la implementación: CGG - GSI - SRHYO

**13. Aspectos de seguridad para la continuidad de la gestión**.

Contemplar los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales todos los aspectos de seguridad de la información involucrada.

Para tal fin se debe:
- identificar las debilidades en los procesos de gestión de información del Organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.
- implementar procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados.
- adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.
- instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.
- recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.

Áreas responsables de la implementación: CGG - GSI

**14. Cumplimiento.**

Cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los

empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.
Para tal fin se debe:

- Identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el Organismo.
- Establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.
- Verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.
- implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

Áreas responsables de la implementación: CGG - GAJ - GA

## 4. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN.

La SSSalud, con el objeto de asignar los roles y funciones necesarios para el Sistema de Gestión de la Seguridad de la Información, cuenta con normas de tipo organizacional, fundamentales para garantizar una adecuada gestión de Seguridad de la Información al interior del Organismo. En ese sentido, la principal instancia responsable de monitorear y gestionar estas normas corresponde al **Comité de Seguridad de la Información**, con el apoyo de las Comisiones y l la Coordinación Técnica de la Gerencia General como área de competencia y del Coordinador asignado como responsable de Seguridad de la Información.

### 4.1. Área responsable de Seguridad de la Información

El área Responsable deberá tener asignada una misión y funciones específicas relacionadas con el Sistema de Gestión de Seguridad de la Información. Asimismo, deberá cumplir y hacer cumplir la presente Política SI y las distintas Normas y Procedimientos que se implementen en la SSSalud.

### 4.2. Comité de Seguridad de la Información

Se debe conformar un Comité de Seguridad de la Información a fin de a establecer un Sistema de Gestión de la Seguridad de la Información y procurar la homogeneidad de criterios para la incorporación de la seguridad de la información en todas las actividades del Organismo, con el objeto de garantizar el acompañamiento manifiesto en el proceso de concientización y el cumplimiento de la presente Política de Seguridad de la Información, con la participación de las áreas sustantivas y de apoyo de la SSSalud. Si bien dicho Comité no es resolutivo, es importante su participación y compromiso a fin de brindar apoyo a las propuestas de Normas y actividades relacionadas con la Seguridad de la Información.

### 4.3. Comisiones de Seguridad de la Información

La conformación de Comisiones Específicas relacionadas con los temas del Sistema de Gestión de Seguridad de la Información, servirán de apoyo tanto al Comité de Seguridad de la información como al Área Responsable de Seguridad de la Información, en todo lo atinente a Normas y buenas prácticas que deban implementarse en la SSSalud.

## 5. ESTRUCTURA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

### 5.1 Agrupamiento Las normas específicas de Seguridad de la Información están agrupadas en tres temas:

#### a. Normas referidas a los Activos de Información y Aspectos Técnicos

La SSSalud, con el objeto de definir los criterios aplicables a los activos de información y las exigencias técnicas de seguridad adecuadas, tiene en desarrollo las normas sobre gestión de activos; seguridad física y ambiental; criptografía; gestión de comunicaciones y operaciones; control de acceso; sobre adquisición, desarrollo y mantenimiento de sistemas de información; gestión de incidentes; y sobre administración de proveedores. (Directrices 4, 6, 7, 8, 9, 10, 12, 13).

#### b. Normas referidas a la Gestión de los Recursos Humanos y Proveedores

La SSSalud, con el objeto de favorecer un uso adecuado de la información y de los sistemas que la apoyan, tiene en desarrollo Normas de Seguridad de la Información vinculadas a la Gestión de Personas y proveedores. Dichas Normas, en la medida que se refieran a obligaciones o prohibiciones que afecten a los empleados de la SSSalud, deberán encontrarse alineadas con la normativa aplicable en la materia. (Directrices 2, 3, 5, 11).

#### c. Normas referidas al Cumplimiento

La SSSalud tiene en desarrollo Normas de Seguridad de la Información asociadas al cumplimiento de disposiciones legales, regulatorias o contractuales. A partir de dichas Normas, se deberán implementar medidas de control que consideren el riesgo legal por incumplimiento, no sólo correctivamente, sino principalmente de forma preventiva. (Directriz 14).

### 5.2 Aprobación y Difusión de las Nomas

Las Nomas específicas de la Seguridad de la Información de SSSalud, así como cualquier modificación a las mismas, deberán ser aprobadas por los estamentos pertinentes, según el contenido, siendo en todos los casos responsabilidad de los niveles gerenciales altos y medios.

Todas las normas de Seguridad de la Información, así como cualquier modificación de la que sean objeto, deberán ser comunicadas a los agentes y funcionarios de la SSSalud de manera pertinente, accesible y comprensible, dejándose constancia de ello.

## 6. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

Integran la presente Política de Seguridad de la Información como Anexo I el Glosario de términos, definiciones y siglas de Seguridad de la Información.

## 7. VIGENCIA Y DIFUSIÓN DE LA POLÍTICA SI

### 7.1 Vigencia

La Política de Seguridad de la Información y todo su contenido tendrá vigencia a partir de su fecha de aprobación y publicación, y tendrá duración indefinida en tanto no se adopte otra resolución al respecto.

### 7.2 Difusión

El texto íntegro y actualizado de la presente Política SI se pondrá y mantendrá a disposición de los interesados en la intranet y en el sitio web de la SSSalud.

# ANEXO I
# GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

# ANEXO I
# GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

**Activo**. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos, que tenga valor para la organización.

**Aceptación de riesgos**: decisión informada de asumir un riesgo particular. La aceptación del riesgo puede surgir sin el tratamiento del riesgo o durante el proceso del tratamiento del riesgo.

**Amenaza**: causa potencial de un incidente no deseado, que puede provocar daños a un sistema, proceso u organización.

**Ambiente de control:** define al conjunto de circunstancias que enmarcan el accionar de una organización desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

**Análisis de riesgo**: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo, incluye la evaluación de riesgos. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones sobre el tratamiento de riesgos.

**Archivo, registro, base o banco de datos**: Indistintamente, designan al conjunto organizado de datos que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

**Ataque**: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso de un activo en forma no autorizada.

**Autenticación**: provisión de garantía de que una característica alegada de una entidad es correcta. Procedimiento que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o es quien dice ser.

**Compartir el riesgo**: Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

**Confidencialidad:** Propiedad que la información pueda ser divulgada o descubierta por usuarios no autorizados, entidades o procesos.

**Competencia**: capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.

**Confiabilidad**: propiedad del comportamiento y resultados previstos consistentes.

**Consecuencia**: resultado de un evento que afecta los objetivos.

Nota: Un evento puede llevar a cabo una serie de consecuencias. Una consecuencia puede ser segura o incierta y, en el contexto de la seguridad de la información, generalmente es negativo.

**Contexto externo**: entorno externo en el que la organización busca alcanzar sus objetivos.

**Nota**: El contexto externo puede incluir lo siguiente:

- lo cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y medio ambiente, ya sea internacional, nacional, regional o local;
- impulsores y tendencias clave que tienen impacto en los objetivos de la organización;

- relaciones y percepciones y valores de partes interesadas externas.

**Contexto interno**: entorno interno en el que la organización busca alcanzar sus objetivos.

**Nota:** El contexto interno puede incluir:

- gobierno, estructura organizativa, roles y responsabilidades;
- políticas, objetivos y las estrategias que existen para lograrlos;
- las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, procesos de información y procesos de toma de decisiones (tanto formales como informales);
- relaciones y percepciones y valores de las partes interesadas internas;
- la cultura de la organización;
- normas, directrices y modelos adoptados por la organización;
- forma y alcance de las relaciones contractuales.

**Continuidad de seguridad de la información**: procesos y procedimientos para controlar operaciones continuas de seguridad de la información.

**Control**: medida que modifica el riesgo. El control consiste en las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer seguridad razonable de que los objetivos de la organización serán alcanzados y que los eventos indeseados serán evitados o bien detectados y corregidos.

**Control de acceso:** significa que el acceso a los activos está autorizado y restringido según el rol y la seguridad.

**Control de Sistemas de Información:** se refiere a todas las políticas, métodos y procedimientos adoptados por una organización para asegurar la protección de su información, la exactitud y confiabilidad de la información y registros de gestión, de la promoción de la eficacia y eficiencia administrativa y adhesión a los estándares de trabajo en la gestión informática.

**Criptografía:** es una disciplina que busca ocultar el contenido semántico o significado de cierta información y de dicha manera proporcionarle confidencialidad, integridad, no repudio y autenticidad.

**Custodios**. Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del área de datos, administradores de sistemas o responsables de un proceso o de un proyecto específico, entre otros.

**Datos informatizados**: Los datos sometidos al tratamiento o procesamiento electrónico o automatizado.

**Datos personales**: Información de cualquier tipo referida a personas humanas o de existencia ideal determinadas o determinables.

**Datos sensibles**: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

**Disconformidad**: incumplimiento de un requisito.

**Disociación de datos**: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

**Disponibilidad:** Propiedad de un activo de ser accesible y utilizable bajo demanda por una entidad autorizada.

**Eficacia**: medida en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

**Evaluación de riesgo:** Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.

La evaluación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.

**Evento**: ocurrencia o cambio de un conjunto particular de circunstancias.

**Nota**: Un evento puede ser una o más ocurrencias y puede tener varias causas; puede consistir en que algo no suceda o un evento a veces puede ser referido como un "incidente" o "accidente".

**Eventos de seguridad de la información:** Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

**Evitar el riesgo**: Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

**Gestión de incidentes de seguridad de la información**: conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de incidentes de seguridad de la información.

**Gestión de riesgos**: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

**Gobierno de la seguridad de la información**: sistema por el cual las actividades de seguridad de la información de una organización están dirigidas y controladas.

**Identificación de riesgo**: proceso de búsqueda, reconocimiento y descripción de riesgos.

La identificación de riesgos implica la identificación de fuentes de riesgo, eventos, sus causas y sus posibles consecuencias. Puede incluir datos históricos, análisis teóricos, opiniones de expertos y las necesidades de los interesados.

**Impacto**: Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

**Incidente**: Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

**Incidente de seguridad:** uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la organización y amenazan a la seguridad de la información.

**Indicador**: medida que proporciona una evaluación o estimación.

**Información documentada**: información requerida para ser controlada y mantenida por una organización y el medio en que está contenido.

Nota: La información documentada puede estar en cualquier formato y medio y desde cualquier fuente.

La información documentada puede referirse a:

- el sistema de gestión, incluidos los procesos relacionados;
- información operativa creada por la organización (documentación);
- evidencia de resultados alcanzados (registros).

**Instalaciones de procesamiento de información**: cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo almacena.

**Integridad:** Propiedad de salvaguardar la precisión y completitud de los activos.

**Llaves criptográficas:** Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

**Medida**: variable a la que se asigna un valor como resultado de la medición.

**Medición**: proceso para determinar un valor.

**Mejora continua**: actividad recurrente para mejorar el rendimiento.

**Necesidad de información**: conocimiento necesario para gestionar objetivos, metas, riesgos y problemas.

**Nivel de riesgo**: magnitud de un riesgo expresado en términos de la combinación de consecuencias y su probabilidad.

**No repudio**: capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.

**Objetivo**: resultado a alcanzar. Un objetivo puede ser estratégico, táctico u operativo.

**Nota**: Los objetivos pueden:

- relacionarse con diferentes disciplinas (como finanzas, salud y seguridad, y objetivos ambientales) y
- ser diferente según los niveles (como estratégico, de toda la organización, proyecto, producto y proceso).
- expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (p. ej. objeto, meta o propósito).

En el contexto de los sistemas de gestión de seguridad de la información, los objetivos son establecidos por la organización, de acuerdo con la política de seguridad de la información, para lograr resultados específicos.

**Objetivo de control**: declaración del resultado a obtener o del propósito a lograr mediante la implementación de procedimientos de control en una actividad particular.

**Política**: intenciones y dirección de una organización, según lo expresado formalmente por su máxima autoridad.

**Probabilidad**: posibilidad de que ocurra algo.

**Proceso**: conjunto de actividades interrelacionadas o interactivas que transforman las entradas en salidas.

**Proceso de gestión de riesgos**: Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicar, consultar, establecer el contexto e identificar, analizar, evaluar, tratar, monitorear y revisar el riesgo.

**Nota**: La ISO/IEC 27005 utiliza el término "*proceso*" para describir la gestión de riesgos en general. Los elementos dentro del proceso de *gestión de riesgos* se denominan "actividades".

**Propietario del riesgo**: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

**Recurso:** Cualquier elemento que tenga valor para la organización.

**Reducir el riesgo**: Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

**Requisito**: Necesidad o expectativa determinada, generalmente implícita u obligatoria. Significa que es una práctica personalizada o común para la organización y partes interesadas, que la necesidad o expectativa bajo esas condiciones está implícita.

**Responsable**: Persona humana de carácter privado que decide sobre el tratamiento de los datos.

**Responsable de archivo, registro, base o banco de datos**: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

**Retención del riesgo**: Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

**Revisión**: actividad realizada para determinar la idoneidad, adecuación y evolución del tema para alcanzar los objetivos establecidos.

**Riesgo**: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad.

**Nota**: El riesgo a menudo se caracteriza por la referencia a posibles "eventos" y "consecuencias" o una combinación de ambos.

El riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la "probabilidad" asociada de ocurrencia.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden ser expresados como efecto de incertidumbre sobre los objetivos de seguridad de la información.

El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causar daño a una organización.

**Riesgo residual**: riesgo restante después del tratamiento de riesgo.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, privacidad, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

**Sistema de administración de la seguridad de la información**: Parte de los sistemas de la organización, basado en el análisis de riesgo, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

**Sistema de gestión**: conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas, normas y procesos para lograr sus objetivos.

**Nota**: Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y asignaciones de la organización, planificación y operación.

El alcance de un sistema de gestión puede incluir a toda la organización o funciones o secciones específicas de la organización.

**Sistema de Gestión de Seguridad de Datos Personales** (SGSDP): Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad,

proporcionalidad y responsabilidad previstos en la Ley N° 25.356, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica estipule en la materia.

**Sistema de información**: conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

**Supervisión**: determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.

**Titular de los datos**: Toda persona física o jurídica cuyos datos sean objeto de tratamiento.

**Tratamiento**: La obtención, uso, divulgación o almacenamiento de datos, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos.

**Tratamiento de datos**: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

**Tratamiento de riesgo**: proceso para modificar el riesgo. El tratamiento del riesgo puede involucrar:

- evitar el riesgo, cuando se decide no comenzar o continuar con la actividad que da lugar al riesgo;
- asumir o aumentar el riesgo, para aprovechar una oportunidad;
- eliminar la fuente de riesgo;
- cambiar la probabilidad;
- cambiar las consecuencias;
- compartir el riesgo con otra parte o partes;
- retener el riesgo por elección de la organización.

**Nota**: El tratamiento de riesgos que tienen consecuencias negativas a veces se denominan "mitigación de riesgo", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos ".

El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

**Usuario de datos**: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos o bases de datos propios o a través de conexión con los mismos.

**Valoración de riesgo:** Evaluación de riesgo a través del análisis de la totalidad de los procesos de la organización.

**Vulnerabilidad**: falta o debilidad de seguridad en un activo o control que puede ser explotado por una o más amenazas.

## SIGLAS

- AG: Asesor de Gabinete
- CO: Coordinación Operativa
- COMITÉ SI: Comité de Seguridad de la Información
- CGG: Coordinación Técnica
- DUSS: Defensoría del Usuario
- GA: Gerencia de Administración
- GAJ: Gerencia de Asuntos Jurídicos)
- GASUSS: Gerencia de Atención y Servicios al Usuario del Sistema de Salud
- GCEF: Gerencia de Control Económico Financiero
- GCP: Gerencia de Control Prestacional
- GDYA: Gerencia de Delegaciones y Articulación de los Integrantes del Sistema de Salud
- GG: Gerencia General
- GGE: Gerencia de Gestión Estratégica
- GOSR: Gerencia Operativa de Subsidios por Reintegros
- GSI: Gerencia de Sistemas de Información
- PROPIETARIO: Propietario de proceso
- RSF: Responsable de Seguridad Física
- SAT: Subgerencia de Asistencia Técnica
- SG: Secretaría General
- SI: Seguridad de la Información
- SRHYO: Subgerencia de Recursos Humanos y Organización
- UAI: Unidad de Auditoría Interna
- UR: Unidad Responsable
- USI: Unidad Superintendencia

### Actualización del documento

| Versión | Revisado por | Contacto | Fecha de revisión | Aprobado por | Cargo | Fecha de aprobación |
|---|---|---|---|---|---|---|
| N° 1.0 | | | | | | |
| N° 1.1 | | | | | | |
| N° 1.2 | | | | | | |

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

**Hoja Adicional de Firmas**
**Informe gráfico**

**Número:** IF-2021-122309374-APN-GG#SSS

CIUDAD DE BUENOS AIRES
Jueves 16 de Diciembre de 2021

**Referencia:** Política SI SSSalud 15-12-2021

---

El documento fue importado por el sistema GEDO con un total de 19 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.12.16 15:49:58 -03:00

Juan Carlos Sturla
Asesor Técnico
Gerencia General
Superintendencia de Servicios de Salud

Digitally signed by Gestion Documental Electronica
Date: 2021.12.16 15:49:58 -03:00