Políticas de Seguridad

**De System Box para la empresa IPM oriente**

**Integrantes:**

Paola Cedeño

Cristhian Medina

Christian Quijada

Christopher Sierra

Jesús Vallenilla

# Tabla de contenido

[Tabla de contenido 2](#_Toc160143467)

[Objetivo 2](#_Toc160143468)

[Alcance 2](#_Toc160143469)

[Glosario 3](#_Toc160143470)

[Aspectos Reglamentarios 5](#_Toc160143471)

[Regulación Externa 5](#_Toc160143472)

[Políticas de Seguridad de la Información 6](#_Toc160143473)

# Objetivo

Formalizar el procedimiento de Gestión de Seguridad de la Información, que forma parte del proceso de Gestión de Riesgos y Control. Definir y reglamentar los procedimientos requeridos para la operación del Sistema Gerencial de Información, con el fin de asegurar que se ejecuten las actividades necesarias para proteger la información de las amenazas que puedan afectarla. Fomentar una cultura orientada a reducir el riesgo de información, lo que permitirá a la entidad mantener el monitoreo, control y medición de las amenazas y vulnerabilidades, y aplicar procedimientos que salvaguarden la confidencialidad, integridad, disponibilidad y privacidad de la información.

# Alcance

Este manual abarca exhaustivamente el proceso completo de gestión de seguridad de la información, desde la conceptualización y formulación de políticas hasta la evaluación y mejora continua del proceso. En este sentido, no solo se limita a la etapa inicial de definición de políticas y planificación, sino que también incluye la implementación práctica de los planes elaborados, su ejecución en el entorno operativo y un monitoreo constante para garantizar su eficacia y adaptabilidad a los cambios.

Se establece como objetivo principal no solo la implementación de las políticas y procedimientos definidos, sino también la mejora continua de todo el proceso de gestión de seguridad de la información. Esto implica la identificación de áreas de oportunidad, la extracción de lecciones aprendidas de la experiencia y la aplicación de prácticas mejoradas de manera sistemática y constante.

Además, se enfoca en la participación activa de todo el personal involucrado en el proceso, promoviendo una cultura organizacional orientada hacia la seguridad de la información y la excelencia operativa. Se busca, por tanto, fomentar un compromiso generalizado con los principios y objetivos de seguridad de la información, así como una comprensión clara de los roles y responsabilidades de cada miembro del equipo en la ejecución y mantenimiento de estos estándares.

# Glosario

**Activo de Información:** Es un dato o elemento que tiene valor para la Entidad. Amenaza: Hecho que puede producir un daño provocado por un evento.

**ASI:** Analista de Seguridad de la Información.

**Auditoría:** Práctica que permite identificar el nivel de cumplimiento y adherencia dentro de la organización a las normas, principios o buenas prácticas de la disciplina que se está analizando.

**Cifrado:** Proceso de convertir información legible en un código secreto para protegerla contra accesos no autorizados

**Confidencialidad:** Seguridad de que la información es accesible solamente por quienes están autorizados para ello.

**Disponibilidad:** Seguridad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando los requieren.

**Dueño de la Información:** Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.

**Evento:** Suceso repentino que puede generar alguna afectación o alarma en un sistema de información.

**Hackeo:** Acción de penetrar ilegalmente en un sistema informático con el propósito de robar información, causar daño o interrumpir su funcionamiento normal.

**Incidente:** Hecho o evento que puede afectar un activo de información.

**Integridad:** Protección de la exactitud, del estado completo de la información y de los métodos de procesamiento.

**Logs:** Registro oficial de eventos durante un período de tiempo en particular. Identifica información sobre quién, qué, cuándo, dónde y por qué un evento ocurre en cualquier sistema de información.

**Malware:** Software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario.

**Nivel de Sensibilidad:** Es un indicador del valor o importancia que la información tiene para la organización, según la clasificación asignada a sus características de integridad, disponibilidad y privacidad.

**Norma:** Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.

**Riesgo:** Es la probabilidad de que ocurra un evento de seguridad. Seguridad física: Consiste en proteger los equipos de procesamiento de la información contra daños físicos, destrucción o robo; también protege las instalaciones designadas para el procesamiento de la información contra daños, destrucción o acceso no autorizado, así como al personal contra situaciones potencialmente dañinas.

**Segregación de Funciones:** Es el principio que regula las funciones de uno o más funcionarios para implementar el principio de doble participación. Estas funciones no deben ser contradictorias ni superponer responsabilidades entre los actores de un procedimiento.

**Seguridad de la Información:** Se refiere a la preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede incluir otras propiedades como autenticidad, trazabilidad, no repudio y afinidad.

**Procedimientos**: Son pasos operativos específicos que los individuos deben seguir para alcanzar los objetivos definidos en las políticas.

**Respaldos (Backups):** Copias de seguridad de los datos almacenados en un sistema, realizadas regularmente para proteger contra pérdidas de datos debido a fallos de hardware, ataques de malware o errores humanos.

# Aspectos Reglamentarios

## Regulación Externa

* Ley Orgánica de Protección de Datos Personales: Esta ley establece los principios, derechos y obligaciones para el tratamiento de datos personales en el país, regulando la recopilación, almacenamiento, uso, circulación y protección de la información personal.
* Ley de Protección al Consumidor y al Usuario: Esta ley protege los derechos de los consumidores y usuarios en transacciones financieras y comerciales, estableciendo mecanismos para la resolución de conflictos y garantizando la calidad de los productos y servicios.

## Políticas de Seguridad de la Información

**Declaración de la Política**

La política de seguridad de la información de las entidades del sector asegurador tiene como objetivo primordial asegurar la protección de los activos de información utilizados en los procesos operativos de la empresa. Esto se logra a través de un equipo capacitado y comprometido con la seguridad de la información, garantizando la continuidad en las 3 operaciones y procesos que respaldan los objetivos del negocio, así como fomentando la mejora continua.

**Objetivos de la Política**

Fortalecer la gestión de seguridad de la información mediante la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Optimizar los procesos estableciendo mecanismos que garanticen la mejora continua. Promover programas de formación y sensibilización del personal en materia de seguridad de la información y continuidad del negocio.

Cultivar y mantener una cultura organizacional en seguridad de la información.

**Alcance de la Política**

La Política de Seguridad de la Información es aplicable a todos los niveles de la empresa: usuarios (funcionarios, accionistas, clientes), terceros (proveedores y contratistas), entes de control y entidades relacionadas que acceden, ya sea interna o externamente, a cualquier activo de información, sin importar su ubicación. Además, esta política se extiende a toda la información corporativa, independientemente del medio, formato, presentación o ubicación.

**Principios de Seguridad**

**Confidencialidad:** Garantizar que la información solo sea accesible, modificada o eliminada por personas autorizadas.

**Disponibilidad:** Asegurar que la información esté disponible siempre que se necesite.

Integridad: Mantener la veracidad y fidelidad de la información a su fuente, sin importar su ubicación o medio de almacenamiento y transmisión.

**Cumplimiento**

La Política de Seguridad de la Información y Continuidad del Negocio, junto con todas las normativas internas, procesos, procedimientos, estándares, controles y directrices derivadas de ella, deben ser cumplidas por todos los implicados, incluyendo funcionarios, miembros, afiliados, clientes, proveedores, entes de control, autoridades administrativas o judiciales, y cualquier persona que acceda a los activos de información. El incumplimiento acarreará las acciones disciplinarias correspondientes.

**Aplicabilidad**

La gestión de la continuidad se enfocará en controlar los riesgos actuales y potenciales de la información, considerando su impacto en las operaciones y objetivos de negocio de la empresa, en línea con la normativa de Seguridad Internacional ISO 27001 y las recomendaciones de los organismos de control y supervisión.

**Compromiso de la Dirección**

La Alta Dirección de la empresa manifiesta su compromiso con la información como uno de sus activos más importantes. Por lo tanto, asegura su total respaldo al establecimiento, 4 implementación y gestión de un Sistema de Seguridad de la Información, que incluye el diseño e implementación de un plan de continuidad y recuperación ante desastres. La Alta Dirección demostrará su compromiso mediante la revisión y aprobación de esta política, su divulgación a todos los funcionarios, y garantizando los recursos necesarios para su implementación y mantenimiento.

**Políticas Específicas de Seguridad de la Información**

En esta sección, se detallan las políticas específicas que están directamente relacionadas con los dominios, objetivos de control y controles establecidos en el Anexo A de la Norma ISO 27001:2013. Estas políticas se encuentran estrechamente vinculadas con la Política General de seguridad de la información y delinean la conducta aceptada por la empresa en el manejo de su información, así como las acciones necesarias para alcanzar los objetivos establecidos en dicha política.

Estas políticas específicas abarcan una variedad de áreas y aspectos relacionados con la seguridad de la información, incluyendo, pero no limitándose a la gestión de accesos, protección de datos, seguridad física, gestión de riesgos, continuidad del negocio y cumplimiento normativo. Cada política establece directrices claras y procedimientos detallados que deben ser seguidos por todos los empleados y partes interesadas para garantizar la adecuada protección de la información y el cumplimiento de los estándares de seguridad establecidos.

Además, estas políticas están diseñadas para adaptarse a las necesidades específicas de la empresa y para asegurar que se apliquen de manera efectiva en todos los niveles de la organización. Se promueve la participación activa y el compromiso de todos los empleados en la implementación y el cumplimiento de estas políticas, con el fin de fortalecer la postura de seguridad de la empresa y proteger sus activos de información de manera integral.

La información que la Entidad utilice para el desarrollo de sus objetivos de negocio debe tener asignado un dueño, quién la utiliza en su área y es el responsable por su correcto uso. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso. Los dueños de la información son los responsables de asegurar que la información del negocio cuente con las políticas para la protección y preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información. El uso de la información de la Entidad por personal de terceros, socios, entidades relacionadas, ya sea local o remotamente, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento del presente Manual. En el contrato de servicios se debe incluir un documento que detalle sus compromisos en el cuidado de la información de la Entidad y las penas a que estarían sujetos en caso de incumplirlos. El cumplimiento de los niveles de servicio en seguridad de la información de terceros, debe ser verificado periódicamente. Cada relación con un tercero debe tener un representante de alto nivel dentro de la misma, que vele por el correcto uso y la protección de la información del negocio. Éste será responsable por la actividad de dichos funcionarios durante la vigencia del contrato. A.6.1.2. Segregación de tareas. Control: los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional de la información de la Entidad, o el uso indebido de los activos de la organización. A.6.1.3. Contacto con las autoridades. Control: se deben mantener los contactos apropiados con las autoridades pertinentes, que pueden apoyar a solucionar conflictos en cuanto a la seguridad de la información de la Entidad. A.6.1.4. Contacto con grupos de interés especial. Control: para la entidad siempre debe ser conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. A.6.1.5. Seguridad de la información en la gestión de proyectos. Control: durante la planeación y ejecución de los proyectos de la Entidad, además de las áreas interesadas, debe participar el área de Seguridad de la Información como generador de recomendaciones en la evaluación de los riesgos inherentes con dichos proyectos. A.6.2. Dispositivos para movilidad y teletrabajo. Objetivo: garantizar la seguridad del teletrabajo y el uso de dispositivos móviles. LOGO EMPRESA POLITICAS DE SEGURIDAD Código: MP-PSI-01 Versión: 1.0 10 A.6.2.1. Política de uso de dispositivos para movilidad. Control: el uso de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Entidad, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Gerencia de Seguridad de la Información y podrá llevarse a cabo sólo en dispositivos provistos por la organización para tal fin. A.6.2.2. Teletrabajo. Control: se debe proteger la información a la que se tiene acceso, que es procesada o almacenada en lugares en los que se realiza teletrabajo. Esta información debe estar encriptada y tener todos los softwares necesarios para protegerla de los ataques. A.7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. A.7.1. Antes de la contratación. Objetivo: asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran. A.7.1.1. Investigación de antecedentes. Control: los nuevos empleados que ingresen a la Entidad, deben pasar por un proceso de investigación de antecedentes, con el fin de mitigar los riesgos en el uso de la información. A.7.1.2. Términos y condiciones de contratación. Control: los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades y los cuidados que deben tener con la información de la Entidad. A.7.2. Durante la contratación. Objetivo: asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. A.7.2.1. Responsabilidades de gestión. Control: la Entidad debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en Seguridad de la Información desde su ingreso hasta su retiro. A.7.2.2. Concienciación, educación y capacitación en seguridad de la información. Control: la Entidad debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros, capacitándolos constantemente en actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. A.7.2.3. Proceso disciplinario. Control: las Políticas de Seguridad de la Información con sus respectivas normas, estándares, procedimientos y demás documentos que se generen y soporten el Sistema de LOGO EMPRESA POLITICAS DE SEGURIDAD Código: MP-PSI-01 Versión: 1.0 11 Gestión de Seguridad de la Información son de obligatorio cumplimiento. La ejecución de acciones que atenten contra la confidencialidad, disponibilidad, integridad y privacidad de la información resultará en una acción disciplinaria que puede llegar hasta la terminación del contrato de trabajo y al posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen. A.7.3. Cese o cambio de puesto de trabajo. Objetivo: proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato. A.7.3.1. Cese o cambio de puesto de trabajo. Control: se debe informar a los empleados o contratistas, las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato, los cuales deben cumplir. A.8. GESTIÓN DE ACTIVOS. A.8.1. Responsabilidad sobre los activos. Objetivo: identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. A.8.1.1. Inventario de activos. Control: la Entidad debe mantener un inventario de recursos o activos de información. Los dueños de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso y/o requerimientos legales de retención. A.8.1.2. Propiedad de los activos. Control: el área responsable del proceso debe realizar el debido control y mantenimiento al inventario de activos de tecnología e información, para establecer responsabilidad sobre la tenencia de los mismos y la información sobre estos, incluido el control al licenciamiento de software. A.8.1.3. Uso aceptable de los activos. Control: independientemente del medio en donde se encuentre cada activo de información, éstos deben ser clasificados por el dueño de la información, mediante el estándar de clasificación establecido. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción. A.8.1.4. Devolución de activos. Control: todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. Debe quedar un acta de dicha devolución, firmada por ambas partes. LOGO EMPRESA POLITICAS DE SEGURIDAD Código: MP-PSI-01 Versión: 1.0 12 A.8.2 Clasificación de la información. Objetivo: asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. A.8.2.1. Directrices de clasificación. Control: Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo con los siguientes criterios: