hackmetrix
ciberseguridad para startups

Política del SGSI

(Sistemas de Gestión de Seguridad de la Información)

Tabla de contenido

1. Objetivo

"Garantizar la protección y la confidencialidad de la información sensible de nuestros clientes, empleados y socios comerciales, reduciendo el riesgo de incidentes de seguridad en un 50% en los próximos 12 meses mediante la implementación de controles de seguridad robustos y la formación continua del personal."

Desglose del Objetivo:

1. **Protección y Confidencialidad de la Información:**
    - Implementar medidas de seguridad para asegurar que la información sensible esté protegida contra accesos no autorizados.
2. **Reducción del Riesgo de Incidentes de Seguridad:**
    - Realizar evaluaciones de riesgos regulares para identificar y mitigar posibles amenazas.
    - Establecer y mantener políticas y procedimientos de seguridad rigurosos.
3. **Implementación de Controles de Seguridad:**
    - Desplegar controles técnicos como cifrado, autenticación multifactor y firewalls.
    - Aplicar controles administrativos como políticas de acceso y gestión de usuarios.
4. **Formación Continua del Personal:**
    - Desarrollar programas de capacitación y concienciación en seguridad de la información para todos los empleados.
    - Realizar simulacros y pruebas de respuesta a incidentes para asegurar que el personal esté preparado para manejar situaciones de seguridad.

Este objetivo debe ser SMART (Específico, Medible, Alcanzable, Relevante y con un Tiempo definido) para asegurar que sea claro y se pueda evaluar su progreso.

El objetivo de este documento es establecer las políticas, prácticas y lineamientos internos aplicable para el Sistema de Gestión de Seguridad de la Información (de ahora en más SGSI) para **[nombreempresa]**.

2.

Alcance

El alcance del SGSI de [Nombre de la Empresa] incluye todas las operaciones y actividades relacionadas con la gestión y protección de la información en los siguientes dominios:

1. **Ámbito Geográfico:**
    - Todas las oficinas, centros de datos y ubicaciones remotas de [Nombre de la Empresa], incluyendo sucursales y oficinas internacionales.
2. **Ámbito Organizativo:**
    - Todas las unidades de negocio y departamentos, incluyendo pero no limitado a:
        - Departamento de TI
        - Departamento de Recursos Humanos
        - Departamento de Finanzas
        - Departamento de Ventas y Marketing
        - Departamento de Operaciones
3. **Ámbito Tecnológico:**
    - Todos los sistemas de información, aplicaciones y bases de datos utilizados por la empresa.
    - Infraestructura de red y telecomunicaciones, incluyendo dispositivos de red, servidores y estaciones de trabajo.
    - Dispositivos móviles y de almacenamiento utilizados para acceder y manejar la información de la empresa.

4. **Ámbito de Procesos:**

   - Procesos de gestión de la información, incluyendo la creación, almacenamiento, transmisión y eliminación de datos.
   - Procesos de gestión de riesgos de seguridad de la información.
   - Procesos de gestión de incidentes de seguridad de la información.

5. **Ámbito de Información:**

   - Toda la información confidencial, sensible y personal manejada por la empresa, incluyendo datos de clientes, empleados y socios comerciales.
   - Documentación y registros relacionados con las operaciones y la gestión de la empresa.

6. **Ámbito Legal y Regulador:**

   - Cumplimiento con todas las leyes, regulaciones y normas aplicables relacionadas con la seguridad de la información y la protección de datos, incluyendo GDPR, HIPAA, y otras regulaciones locales e internacionales pertinentes.

Exclusiones:

- Sistemas y procesos no directamente gestionados o controlados por [Nombre de la Empresa], como los servicios en la nube gestionados por terceros fuera del control contractual.

Este alcance define claramente los límites y las inclusiones del SGSI, asegurando que todas las áreas críticas de la empresa estén cubiertas por las políticas y controles de seguridad de la información.

3.
Vigencia

Su vigencia será a partir de 17/07/24

4.
Responsabilidades

1. Director de Seguridad de la Información (CISO)

Responsabilidades:

- Desarrollar y mantener la estrategia de seguridad de la información.
- Supervisar la implementación y operación del SGSI.
- Asegurar el cumplimiento con las normativas y regulaciones de seguridad de la información.
- Reportar el estado de la seguridad de la información a la alta dirección.

2. Responsable del SGSI

Responsabilidades:

- Coordinar la implementación y mantenimiento del SGSI.
- Realizar evaluaciones de riesgos y gestionar el tratamiento de riesgos.
- Desarrollar y actualizar políticas, procedimientos y controles de seguridad.
- Monitorear y revisar el desempeño del SGSI.

3. Comité de Seguridad de la Información

Responsabilidades:

- Revisar y aprobar las políticas y procedimientos de seguridad.
- Evaluar los riesgos y el impacto en la organización.
- Tomar decisiones sobre la gestión de incidentes y la mejora continua del SGSI.

4. Gerente de TI

Responsabilidades:

- Implementar y gestionar las medidas técnicas de seguridad.
- Asegurar la disponibilidad y la integridad de los sistemas y datos.
- Coordinar con el CISO y el responsable del SGSI para asegurar la alineación con las políticas de seguridad.

5. Responsable de la Gestión de Riesgos

Responsabilidades:

- Identificar, evaluar y priorizar los riesgos de seguridad de la información.
- Desarrollar planes de tratamiento de riesgos y supervisar su implementación.
- Revisar y actualizar periódicamente el análisis de riesgos.

6. Responsable de la Gestión de Incidentes

Responsabilidades:

- Desarrollar y mantener los procedimientos de respuesta a incidentes.
- Coordinar la respuesta a incidentes de seguridad.
- Realizar análisis post-incidente y proponer medidas de mejora.

7. Responsable de la Continuidad del Negocio

Responsabilidades:

- Desarrollar y mantener el plan de continuidad del negocio y recuperación ante desastres.
- Coordinar las pruebas y simulacros del plan de continuidad.
- Asegurar que los planes de continuidad estén alineados con los requisitos del SGSI.

8. Responsable de Cumplimiento

Responsabilidades:

- Asegurar el cumplimiento de las políticas internas y regulaciones externas de seguridad de la información.
- Realizar auditorías internas y externas del SGSI.
- Reportar los hallazgos de auditoría y coordinar las acciones correctivas.

9. Responsable de Formación y Concienciación

Responsabilidades:

- Desarrollar programas de formación y concienciación en seguridad de la información.
- Realizar sesiones de capacitación para empleados y contratistas.
- Evaluar la efectividad de los programas de formación y ajustar según sea necesario.

10. Usuarios Finales

Responsabilidades:

- Cumplir con las políticas y procedimientos de seguridad de la información.
- Reportar incidentes de seguridad y vulnerabilidades.
- Participar en las formaciones y programas de concienciación sobre seguridad.

Estas responsabilidades aseguran que cada aspecto del SGSI esté cubierto y que haya una clara asignación de tareas y responsabilidades dentro de la organización, fomentando una cultura de seguridad de la información integral y colaborativa.

5.
Autoridad de emisión, revisión y publicación

1. Autoridad de Emisión

Responsable: Director de Seguridad de la Información (CISO)

Responsabilidades:

- Aprobar la emisión de nuevas políticas, procedimientos y documentos relacionados con el SGSI.
- Asegurar que todos los documentos cumplan con los requisitos legales y normativos.
- Validar que los documentos reflejen las necesidades y objetivos de la organización.

2. Autoridad de Revisión

Responsable: Comité de Seguridad de la Información

Responsabilidades:

- Revisar periódicamente los documentos del SGSI para asegurar su vigencia y efectividad.
- Proponer modificaciones y mejoras a las políticas y procedimientos existentes.
- Evaluar el impacto de cambios en el entorno normativo, tecnológico y operativo en los documentos del SGSI.

3. Autoridad de Publicación

Responsable: Responsable del SGSI

Responsabilidades:

- Publicar y distribuir los documentos del SGSI a todas las partes interesadas.
- Mantener un registro actualizado de todas las versiones de los documentos.
- Asegurar que los documentos sean fácilmente accesibles para el personal autorizado.

Proceso de Gestión Documental

1. Emisión

- **Paso 1:** El responsable de la emisión (CISO) redacta o actualiza el documento.
- **Paso 2:** El documento es revisado internamente por el equipo de seguridad de la información.
- **Paso 3:** El documento es enviado al Comité de Seguridad de la Información para su revisión.

2. Revisión

- **Paso 4:** El Comité de Seguridad de la Información revisa el documento, propone cambios si es necesario y lo aprueba.
- **Paso 5:** En caso de modificaciones significativas, el documento puede ser revisado nuevamente por el CISO antes de su aprobación final.

3. Publicación

- **Paso 6:** El Responsable del SGSI publica el documento en el repositorio oficial de documentos del SGSI.
- **Paso 7:** Se notifica a todas las partes interesadas sobre la nueva publicación o actualización del documento.
- **Paso 8:** Se mantiene un registro de versiones y un historial de cambios del documento.

6. Términos y definiciones

1. **Activo de Información**
    - **Definición: Cualquier información, dato o sistema que tenga valor para la organización y necesite protección.**
    - **Ejemplo: Bases de datos de clientes, documentos financieros, servidores.**
2. **Amenaza**
    - **Definición: Cualquier circunstancia o evento con el potencial de causar daño a un sistema de información.**
    - **Ejemplo: Malware, ataques de hackers, desastres naturales.**
3. **Autenticación**
    - **Definición: Proceso de verificar la identidad de un usuario, dispositivo o entidad.**
    - **Ejemplo: Uso de contraseñas, tarjetas inteligentes, huellas digitales.**
4. **Confidencialidad**
    - **Definición: Propiedad de la información que asegura que solo las personas autorizadas puedan acceder a ella.**
    - **Ejemplo: Cifrado de datos sensibles.**

5. **Control de Acceso**
    - **Definición: Mecanismos y políticas que regulan quién puede acceder a los recursos de información y bajo qué condiciones.**
    - **Ejemplo: Listas de control de acceso (ACL), autenticación multifactor (MFA).**
6. **Disponibilidad**
    - **Definición: Propiedad de la información que asegura que los usuarios autorizados tienen acceso a ella y a sus recursos asociados cuando sea necesario.**
    - **Ejemplo: Sistemas de respaldo y recuperación ante desastres.**
7. **Integridad**
    - **Definición: Propiedad de la información que asegura que los datos no han sido alterados de manera no autorizada.**
    - **Ejemplo: Firmas digitales, controles de versiones.**
8. **Incidente de Seguridad de la Información**
    - **Definición: Evento o serie de eventos no deseados o inesperados que comprometen la seguridad de la información.**
    - **Ejemplo: Robo de datos, acceso no autorizado a sistemas, infecciones de malware.**
9. **Riesgo**
    - **Definición: Potencial de que una amenaza explote una vulnerabilidad y cause daño a los activos de información.**

- **Ejemplo: Riesgo de fuga de datos debido a contraseñas débiles.**

10. **SGSI (Sistema de Gestión de Seguridad de la Información)**

    - **Definición: Conjunto de políticas, procedimientos y controles implementados para gestionar y proteger la información sensible de una organización.**

    - **Ejemplo: Implementación de la norma ISO/IEC 27001.**

11. **Vulnerabilidad**

    - **Definición: Debilidad en un sistema o proceso que puede ser explotada por una amenaza para causar un incidente de seguridad.**

    - **Ejemplo: Software desactualizado, configuraciones de seguridad incorrectas.**

12. **Política de Seguridad de la Información**

    - **Definición: Documento formal que define el enfoque y los objetivos de la organización en cuanto a la gestión de la seguridad de la información.**

    - **Ejemplo: Políticas de uso aceptable, políticas de privacidad.**

13. **Plan de Continuidad del Negocio (BCP)**

    - **Definición: Plan que detalla los procedimientos y acciones a seguir para mantener las operaciones críticas de la organización en caso de un desastre o interrupción significativa.**

    - **Ejemplo: Procedimientos de respaldo de datos, planes de recuperación de sitios alternativos.**

14. **Plan de Recuperación ante Desastres (DRP)**

    - **Definición: Plan que describe cómo una organización recuperará y restaurará sus funciones tecnológicas después de una interrupción significativa.**
    - **Ejemplo: Procedimientos para restaurar sistemas desde copias de seguridad.**

15. **Auditoría de Seguridad de la Información**

    - **Definición: Proceso de evaluación independiente de los controles de seguridad de la información para asegurar que cumplen con las políticas, procedimientos y normativas.**
    - **Ejemplo: Auditorías internas y externas de conformidad con la norma ISO/IEC 27001.**

16. **Evaluación de Riesgos**

    - **Definición: Proceso de identificación, análisis y evaluación de riesgos para determinar las medidas de control necesarias.**
    - **Ejemplo: Análisis de impacto de riesgos, matrices de riesgos.**

17. **Tratamiento de Riesgos**

    - **Definición: Proceso de selección y aplicación de medidas para mitigar o gestionar los riesgos identificados.**
    - **Ejemplo: Implementación de controles de seguridad, aceptación del riesgo residual.**

18. **Cumplimiento**

    - **Definición: Aseguramiento de que la organización sigue todas las leyes, regulaciones y normas aplicables.**

    - **Ejemplo: Cumplimiento con GDPR, HIPAA, y otras regulaciones relevantes.**

19. **Responsabilidad**

    - **Definición: Deber de los individuos y las organizaciones de asegurar que sus acciones cumplan con los principios y políticas de seguridad de la información.**

    - **Ejemplo: Responsabilidad del CISO en la implementación del SGSI.**

Estos términos y definiciones proporcionan una base común para entender y gestionar la seguridad de la información dentro de una organización, asegurando que todos los miembros estén alineados en cuanto a conceptos y prácticas.

7.
Reglas de aplicación al SGSI

7.1 Comprender la organización y su contexto

Identificación del Contexto Externo e Interno

Para establecer un SGSI eficaz, es crucial comprender tanto el contexto externo como el interno de la organización. Esto incluye factores que pueden afectar su capacidad para alcanzar los objetivos de seguridad de la información.
Contexto Externo:

- Factores Políticos: Legislación y regulaciones locales, nacionales e internacionales aplicables a la seguridad de la información.
- Factores Económicos: Condiciones económicas que pueden influir en los recursos disponibles para la seguridad de la información.
- Factores Sociales: Expectativas y requisitos de los clientes, empleados y otras partes interesadas en cuanto a la protección de la información.
- Factores Tecnológicos: Avances tecnológicos, nuevas amenazas y vulnerabilidades, y cambios en la infraestructura tecnológica.
- Factores Ambientales: Desastres naturales y eventos ambientales que pueden impactar la seguridad de la información.

Contexto Interno:

- Estructura Organizativa: Organigrama, roles y responsabilidades relacionados con la seguridad de la información.
- Cultura Organizativa: Valores, creencias y actitudes hacia la seguridad de la información dentro de la organización.
- Recursos Disponibles: Personal, tecnología, presupuesto y otros recursos asignados a la seguridad de la información.
- Procesos y Procedimientos: Procesos internos y procedimientos operativos que afectan la gestión de la seguridad de la información.
- Interdependencias: Relaciones con terceros, proveedores, socios y otras partes que pueden influir en la seguridad de la información.

Análisis de las Partes Interesadas
Identificar y comprender las necesidades y expectativas de las partes interesadas es fundamental para el SGSI. Las partes interesadas pueden incluir:

- Clientes: Exigen la protección de sus datos personales y confidenciales.
- Empleados: Requieren un entorno seguro para desempeñar sus funciones.
- Socios Comerciales: Esperan que la organización mantenga la integridad y confidencialidad de la información compartida.
- Reguladores: Imponen requisitos legales y normativos que la organización debe cumplir.

- Proveedores: Necesitan garantizar la seguridad en la cadena de suministro de información.

Determinación del Alcance del SGSI

El alcance del SGSI debe estar claramente definido y alineado con el contexto de la organización. Esto incluye:

- Definir los Límites y Alcances: Especificar las ubicaciones, sistemas, procesos y datos que estarán cubiertos por el SGSI.
- Identificar las Exclusiones: Determinar cualquier área que no esté incluida en el SGSI y justificar estas exclusiones.

Identificación de Requisitos de Seguridad de la Información

Es esencial identificar los requisitos de seguridad de la información derivados del contexto interno y externo, así como de las partes interesadas. Estos requisitos pueden incluir:

- Requisitos Legales y Regulatorios: Cumplimiento con leyes y regulaciones específicas, como GDPR, HIPAA, etc.
- Requisitos Contractuales: Cumplimiento con términos y condiciones acordados con clientes y proveedores.
- Requisitos Empresariales: Necesidades internas de la organización para proteger sus activos de información.
- Requisitos de Seguridad de las Partes Interesadas: Expectativas de clientes, empleados y otras partes interesadas en cuanto a la seguridad de la información.

Análisis de Riesgos de Seguridad de la Información

Realizar un análisis de riesgos es fundamental para comprender las amenazas, vulnerabilidades y el impacto potencial en los activos de información de la organización. Este análisis incluye:

- Identificación de Activos: Catalogar los activos de información críticos para la organización.
- Identificación de Amenazas y Vulnerabilidades: Evaluar las amenazas potenciales y las vulnerabilidades asociadas a los activos de información.
- Evaluación del Impacto: Determinar el impacto potencial de la explotación de vulnerabilidades por parte de las amenazas.
- Establecimiento de Medidas de Control: Implementar controles para mitigar los riesgos identificados.

Este enfoque holístico para comprender la organización y su contexto asegura que el SGSI esté alineado con los objetivos estratégicos de la organización y las expectativas de las partes interesadas, proporcionando una base sólida para la gestión de la seguridad de la información.

7.1.1 Declaración de Objetivos

Comentado [1]: Es importante que este alineado y que pueda ser demostrable.

La organización declara los siguientes objetivos de seguridad de la información alineados a la estrategia establecida en el Plan Estratégico de **MEDIREC**.

Objetivo General

Proteger la confidencialidad, integridad y disponibilidad de la información gestionada por [Nombre de la Empresa], garantizando el cumplimiento de todas las leyes y regulaciones aplicables, y asegurando la confianza de nuestros clientes, empleados y socios comerciales.

Objetivos Específicos

1. **Confidencialidad de la Información:**
   - **Objetivo:** Asegurar que la información sensible y crítica sea accesible únicamente por personal autorizado.
   - **Meta:** Implementar controles de acceso robustos y autenticación multifactor para el 100% de los sistemas críticos antes del final del año fiscal.
   - **Indicador de Éxito:** Reducción de incidentes de acceso no autorizado en un 90%.
2. **Integridad de los Datos:**
   - **Objetivo:** Garantizar que los datos almacenados, procesados y transmitidos sean precisos, completos y no hayan sido alterados de manera no autorizada.
   - **Meta:** Implementar mecanismos de verificación y auditoría de integridad de datos en todos los sistemas críticos antes del próximo trimestre.
   - **Indicador de Éxito:** Cero incidentes reportados de alteración no autorizada de datos.
3. **Disponibilidad de los Sistemas:**
   - **Objetivo:** Asegurar que los sistemas y servicios de información estén disponibles para los usuarios autorizados cuando los necesiten.
   - **Meta:** Implementar y probar planes de continuidad del negocio y recuperación ante desastres para todos los servicios críticos antes de fin de año.
   - **Indicador de Éxito:** Mantener una disponibilidad de sistemas críticos del 99.9%.
4. **Cumplimiento Normativo:**
   - **Objetivo:** Cumplir con todas las leyes, regulaciones y normas de seguridad de la información aplicables.
   - **Meta:** Realizar auditorías internas y externas anuales y corregir todas las no conformidades dentro de los 30 días siguientes a la auditoría.
   - **Indicador de Éxito:** 100% de cumplimiento en auditorías de seguridad y normativas.
5. **Gestión de Incidentes de Seguridad:**
   - **Objetivo:** Detectar, responder y mitigar incidentes de seguridad de manera efectiva y oportuna.
   - **Meta:** Implementar un sistema automatizado de gestión de incidentes y capacitar a todo el personal relevante en su uso antes de fin de año.
   - **Indicador de Éxito:** Reducción del tiempo de respuesta a incidentes en un 50%.
6. **Formación y Concienciación:**
   - **Objetivo:** Incrementar la concienciación y las competencias en seguridad de la información entre todos los empleados.
   - **Meta:** Realizar sesiones de formación semestrales y enviar boletines de concienciación trimestrales.
   - **Indicador de Éxito:** 95% de los empleados completan la formación obligatoria en seguridad de la información.

7. **Gestión de Riesgos:**
    - **Objetivo:** Identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información de manera proactiva.
    - **Meta:** Realizar evaluaciones de riesgos semestrales y actualizar el plan de tratamiento de riesgos en consecuencia.
    - **Indicador de Éxito:** Mitigación del 100% de los riesgos críticos identificados.
8. **Protección de Datos Personales:**
    - **Objetivo:** Garantizar la protección de los datos personales en cumplimiento con las leyes de privacidad y protección de datos.
    - **Meta:** Implementar procesos de anonimización y cifrado para todos los datos personales sensibles antes del próximo semestre.
    - **Indicador de Éxito:** Cero incidentes de brechas de datos personales.

Compromiso de la Alta Dirección

La alta dirección de [Nombre de la Empresa] se compromete a proporcionar los recursos necesarios para implementar y mantener el SGSI, apoyando continuamente las iniciativas de seguridad de la información y promoviendo una cultura de seguridad dentro de la organización.

Esta declaración de objetivos proporciona una guía clara y medible para la implementación y gestión del SGSI, asegurando que todos los esfuerzos estén alineados con la misión y visión de la organización.

7.1.2 Contexto de SGSI

Comentado [2]: Cubre 4.1 Comprender la organización y su contexto de la ISO/IEC 27001

1. Comprensión de la Organización y su Contexto

Contexto Externo:

1. **Factores Políticos y Regulatorios:**
    - Cumplimiento con leyes y regulaciones nacionales e internacionales de protección de datos y privacidad (por ejemplo, GDPR, HIPAA).
    - Normativas específicas del sector al que pertenece la organización (por ejemplo, PCI-DSS para el sector financiero).
2. **Factores Económicos:**
    - Condiciones económicas que afectan la disponibilidad de recursos para la inversión en seguridad de la información.
    - Presiones de mercado que impulsan la necesidad de proteger la información para mantener la competitividad.
3. **Factores Sociales:**
    - Expectativas de los clientes y partes interesadas en cuanto a la protección de su información personal y confidencial.
    - Impacto de las redes sociales y la comunicación digital en la percepción de la seguridad y la reputación de la organización.

4. **Factores Tecnológicos:**
    - Evolución constante de las tecnologías de la información y las comunicaciones.
    - Nuevas amenazas y vulnerabilidades emergentes en el entorno digital.
5. **Factores Ambientales:**
    - Riesgos ambientales como desastres naturales que podrían afectar la infraestructura de TI y la continuidad del negocio.
    - Consideraciones de sostenibilidad y eficiencia energética en la gestión de los centros de datos.

Contexto Interno:

1. **Estructura Organizativa:**
    - Organigrama de la organización, roles y responsabilidades relacionados con la seguridad de la información.
    - Existencia de un Comité de Seguridad de la Información y un CISO (Chief Information Security Officer) o equivalente.
2. **Cultura Organizativa:**
    - Valores, creencias y actitudes hacia la seguridad de la información dentro de la organización.
    - Nivel de concienciación y formación en seguridad de la información entre los empleados.
3. **Recursos Disponibles:**
    - Personal especializado en seguridad de la información.
    - Presupuesto asignado para iniciativas de seguridad de la información.
    - Herramientas y tecnologías disponibles para la gestión de la seguridad.
4. **Procesos y Procedimientos:**
    - Procesos internos y procedimientos operativos que afectan la gestión de la seguridad de la información.
    - Existencia de políticas y procedimientos documentados y actualizados.
5. **Interdependencias:**
    - Relaciones con terceros, proveedores, socios y otras partes que pueden influir en la seguridad de la información.
    - Contratos y acuerdos de nivel de servicio (SLA) que incluyen requisitos de seguridad.

2. Análisis de las Partes Interesadas

Identificación y análisis de las partes interesadas, incluyendo sus necesidades y expectativas en relación con la seguridad de la información:

1. **Clientes:**
    - Necesidad de protección de sus datos personales y confidenciales.
    - Expectativas de transparencia y respuesta ante incidentes de seguridad.
2. **Empleados:**
    - Necesidad de un entorno de trabajo seguro.
    - Formación y concienciación en seguridad de la información.
3. **Socios Comerciales y Proveedores:**
    - Expectativas de cumplimiento de estándares de seguridad en la cadena de suministro.
    - Requisitos contractuales relacionados con la seguridad de la información.
4. **Reguladores y Entidades Gubernamentales:**
    - Cumplimiento con leyes y regulaciones aplicables.
    - Obligaciones de reporte y auditoría.
5. **Accionistas e Inversores:**
    - Protección de la reputación y los activos de la empresa.
    - Gestión adecuada de los riesgos de seguridad de la información.

3. Determinación del Alcance del SGSI

Definición clara del alcance del SGSI, especificando las ubicaciones, sistemas, procesos y datos que estarán cubiertos:

1. **Ámbito Geográfico:**
    - Sedes principales y oficinas regionales.
    - Centros de datos y ubicaciones de almacenamiento de información.
2. **Ámbito Tecnológico:**
    - Sistemas de TI y aplicaciones críticas.
    - Infraestructura de red y comunicaciones.
3. **Ámbito de Procesos:**
    - Procesos de negocio críticos que manejan información sensible.
    - Procedimientos operativos y administrativos relacionados con la seguridad de la información.

4. **Ámbito de Datos:**
    - Tipos de información y datos sensibles incluidos en el SGSI.
    - Bases de datos y repositorios de información.

4. Identificación de Requisitos de Seguridad de la Información

Identificación de los requisitos de seguridad de la información derivados del contexto interno y externo, así como de las partes interesadas:

1. **Requisitos Legales y Regulatorios:**
    - Cumplimiento con leyes y normativas de protección de datos y privacidad.
    - Requisitos específicos del sector.
2. **Requisitos Contractuales:**
    - Cláusulas de seguridad en contratos con clientes y proveedores.
    - Acuerdos de nivel de servicio (SLA) que incluyen requisitos de seguridad.
3. **Requisitos Empresariales:**
    - Necesidades internas para proteger los activos de información.
    - Estrategias de negocio que dependen de la seguridad de la información.
4. **Requisitos de Seguridad de las Partes Interesadas:**
    - Expectativas de clientes, empleados y otras partes interesadas en cuanto a la protección de la información.
    - Necesidades de transparencia y respuesta ante incidentes de seguridad.

5. Evaluación y Tratamiento de Riesgos

Realización de una evaluación de riesgos para identificar, analizar y mitigar los riesgos relacionados con la seguridad de la información:

1. **Identificación de Activos:**
    - Catalogación de los activos de información críticos.
    - Identificación de propietarios de activos.
2. **Identificación de Amenazas y Vulnerabilidades:**
    - Evaluación de amenazas potenciales y vulnerabilidades asociadas a los activos de información.
    - Análisis de escenarios de riesgo.
3. **Evaluación del Impacto:**
    - Determinación del impacto potencial de la explotación de vulnerabilidades por parte de las amenazas.
    - Clasificación de riesgos según su impacto y probabilidad.

4. **Establecimiento de Medidas de Control:**
    - Implementación de controles de seguridad para mitigar los riesgos identificados.
    - Revisión y mejora continua de las medidas de control.

Este enfoque asegura que el SGSI esté alineado con los objetivos estratégicos de la organización y las expectativas de las partes interesadas, proporcionando una base sólida para la gestión de la seguridad de la información.

Análisis externo

El contexto externo incluye cualquier cosa dentro de la organización que pueda influir en la forma en que una organización administra su riesgo de seguridad de la información.

Político Política gubernamental	**Económico** Economía y finanzas	**Social** Cultura	**Tecnológico** Avances e innovación	**Legal** Leyes y regulaciones
La política gubernamental juega un papel crucial en la regulación y protección de la información y la seguridad cibernética. Las leyes y regulaciones establecidas por el gobierno pueden influir significativamente en las prácticas de seguridad de la información de las organizaciones. Es fundamental para las empresas estar al tanto de las normativas vigentes, como GDPR en Europa o HIPAA en Estados Unidos, y adaptar sus políticas y procedimientos de seguridad de acuerdo con estas normativas para cumplir con las obligaciones legales y proteger los datos de manera efectiva.	El entorno económico y financiero en el que opera una empresa puede tener un impacto significativo en sus estrategias y operaciones relacionadas con la seguridad de la información. Factores económicos como la disponibilidad de recursos financieros pueden influir en la capacidad de la empresa para invertir en tecnologías y controles de seguridad robustos. Además, la estabilidad económica y las condiciones del mercado pueden afectar la demanda de productos y servicios, así como la priorización de iniciativas de seguridad de la información.	El análisis cultural externo considera las normas, valores y actitudes compartidas en la sociedad. Estos factores pueden influir en cómo se percibe y gestiona la seguridad de la información dentro de una organización, afectando las políticas y prácticas de privacidad, confidencialidad, educación y adopción tecnológica.	El entorno de avances e innovación externos incluye los desarrollos tecnológicos y las tendencias emergentes que pueden impactar la seguridad de la información de una organización. Estos avances pueden proporcionar nuevas herramientas y métodos para mejorar la protección de datos y la gestión de riesgos cibernéticos. Es crucial para las empresas mantenerse al tanto de estos avances para adaptar sus estrategias de seguridad de la información y mantenerse competitivas en un entorno digital en constante evolución.	Las leyes y regulaciones externas son fundamentales para la seguridad de la información de una empresa. Normativas como GDPR en Europa, HIPAA en Estados Unidos, y otras leyes de protección de datos a nivel global establecen estándares y requisitos específicos que las organizaciones deben cumplir. Estas regulaciones pueden influir en las políticas y prácticas de seguridad de la información, afectando cómo se recopilan, almacenan, procesan y protegen los datos personales y confidenciales. Es esencial para las empresas estar al tanto de estas leyes y adaptar sus procesos de seguridad para cumplir con los requisitos legales y mitigar riesgos de incumplimiento.

Análisis interno

El contexto interno incluye cualquier cosa dentro de la organización que pueda influir en la forma en que una organización administra su riesgo de seguridad de la información.

Fortalezas	Debilidades
Personal con experiencia y capacitación sólida en seguridad de la información. Expertos en tecnologías emergentes y herramientas de seguridad. Alta conciencia y compromiso de los empleados hacia las prácticas de seguridad de la información. Procesos establecidos para la gestión de incidentes y respuesta ante crisis. Sistemas de última generación y redes seguras. Implementación de controles de acceso físico y lógico efectivos.	Limitaciones presupuestarias para inversiones en tecnología de seguridad avanzada. Necesidad de optimización de costos sin comprometer la seguridad. Dificultades para cumplir con múltiples regulaciones globales y sectoriales. Complejidad en la gestión y actualización de políticas de seguridad de la información. Vulnerabilidades relacionadas con terceros y proveedores en la cadena de suministro. Falta de control total sobre la seguridad de servicios y productos externos.
Oportunidades	**Amenazas**
Aumento de la demanda de soluciones de seguridad cibernética debido a amenazas emergentes. Oportunidades para expandir servicios de consultoría y gestión de seguridad. Innovaciones en inteligencia artificial y análisis de datos para mejorar la detección de amenazas. Desarrollo de soluciones de seguridad más eficientes y económicas. Posibilidad de ingresar a nuevos mercados con requisitos específicos de seguridad de la información. Alianzas estratégicas internacionales para compartir mejores prácticas y tecnologías.	Incremento de amenazas como ransomware y phishing dirigido. Potencial de pérdida de datos críticos y daño a la reputación de la empresa. Actualizaciones frecuentes en leyes de privacidad y protección de datos que requieren ajustes continuos. Riesgo de sanciones y multas por incumplimiento de normativas. Presión competitiva de empresas establecidas y nuevas entrantes en el mercado de seguridad cibernética. Necesidad de diferenciación y oferta de valor agregado para retener clientes y atraer nuevos.

7.1.3 Contexto de Gestión de Riesgos

1. Identificación de Activos Críticos:

- **Datos Sensibles:** Información de clientes, datos financieros y estrategias comerciales almacenadas en sistemas CRM y ERP.
- **Infraestructura de TI:** Servidores, redes y aplicaciones críticas para la operación diaria.

2. Evaluación de Amenazas y Vulnerabilidades:

- **Amenazas:** Ciberataques, malware, vulnerabilidades de software y hardware.
- **Vulnerabilidades:** Falta de parches de seguridad actualizados, acceso no autorizado debido a contraseñas débiles.

3. Valoración de Impacto:

- **Impacto Potencial:** Pérdida de datos sensibles, interrupción de servicios críticos, daño a la reputación de la empresa, posibles sanciones regulatorias.

4. Análisis de Riesgos:

- **Riesgos Priorizados:** Ciberataques dirigidos a datos sensibles, falta de capacitación adecuada del personal en seguridad de la información.

5. Selección y Aplicación de Controles:

- **Controles Implementados:**
  - Seguridad perimetral mejorada con firewalls avanzados y sistemas de detección de intrusiones.
  - Políticas estrictas de gestión de contraseñas y autenticación multifactor.
  - Capacitación continua del personal en concienciación sobre seguridad.

6. Monitoreo y Revisión Continua:

- **Prácticas de Monitoreo:** Auditorías regulares de seguridad, evaluaciones de vulnerabilidades, pruebas de penetración y simulacros de incidentes.
- **Revisión y Mejora:** Actualización continua de políticas y procedimientos según las nuevas amenazas y cambios en el entorno regulatorio.

7.2 Comprender las necesidades y expectativas de las partes interesadas

Comentado [3]: Cubre 4.2

1. Identificación de Partes Interesadas:

- **Clientes:** Expectativas de productos de calidad, servicio al cliente eficiente y protección de datos personales.
- **Empleados:** Ambiente de trabajo seguro, oportunidades de desarrollo profesional y concienciación en seguridad laboral.
- **Accionistas:** Rendimiento financiero sostenible, transparencia en la gestión y cumplimiento de regulaciones.
- **Proveedores:** Relaciones comerciales justas, pagos oportunos y cumplimiento de normativas de seguridad de la información.
- **Reguladores y Gobierno:** Cumplimiento estricto de leyes y regulaciones, informes transparentes y responsabilidad corporativa.
- **Comunidad Local:** Contribución social responsable, impacto ambiental mínimo y relaciones comunitarias positivas.

2. Evaluación de Necesidades y Expectativas:

- **Clientes:** Encuestas de satisfacción, análisis de reclamaciones y comentarios en redes sociales para entender preferencias y preocupaciones.
- **Empleados:** Encuestas internas de clima laboral, programas de desarrollo profesional y sesiones de formación en seguridad y salud laboral.
- **Accionistas:** Informes financieros detallados, reuniones de accionistas y comunicación regular sobre estrategias y desempeño corporativo.
- **Proveedores:** Encuestas de satisfacción de proveedores, evaluaciones de cumplimiento y auditorías para asegurar estándares de seguridad de la información.
- **Reguladores y Gobierno:** Revisión y cumplimiento continuo de leyes locales e internacionales, participación activa en consultas públicas y actualización de políticas internas.
- **Comunidad Local:** Programas de responsabilidad social corporativa, eventos comunitarios patrocinados y gestión proactiva de impactos ambientales.

3. Implementación de Estrategias y Acciones:

- **Personalización de Servicios:** Adaptación de productos y servicios según las preferencias del cliente identificadas.
- **Programas de Bienestar:** Implementación de políticas de bienestar laboral, formación en seguridad y salud ocupacional y programas de desarrollo profesional.

- **Transparencia y Rendición de Cuentas:** Publicación de informes anuales detallados, reuniones regulares con accionistas y comunicación clara sobre políticas y desempeño corporativo.
- **Colaboración con Proveedores:** Establecimiento de estándares de seguridad de la información, compromisos contractuales claros y evaluaciones periódicas de desempeño.
- **Cumplimiento Normativo:** Establecimiento de comités de cumplimiento, auditorías internas y formación continua en leyes y regulaciones vigentes.
- **Iniciativas Comunitarias:** Asociaciones con organizaciones locales, patrocinio de eventos y programas de voluntariado para mejorar la calidad de vida en la comunidad.

7.2.1. Identificación y Análisis de las Partes Interesadas

Categoría	Interesados detectados
Personal Interno	Gerente General - CEO
	Miembros del Directorio (si aplica)
	Comité de Seguridad de Información
	Oficial de Seguridad / Coordinador de Seguridad
	Jefaturas de los Procesos/Servicios
	Personal Operativo de los Procesos
Personas Externas	Clientes
	Inversionistas
	Usuarios finales (si aplica)

Proveedores	Proveedores de Personal Tercerizado (si aplica)
	Proveedores de Servicios
	Proveedores de Tecnologías: Servidores en la nube, Sistemas de Alarma Ambiental, Máquinas Virtuales, Software de Monitoreo, Software de Gestión de TI, Certificados Digitales.

7.2.2. Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas

Identificación de requisitos de CLIENTES

- Entregar productos y servicios con soporte y mantenimiento:
  - de acuerdo con los requisitos contractuales,
  - en caso de interrupciones,
  - cumpliendo los requisitos legales aplicables,
  - cumpliendo los requisitos adicionales de la industria aplicables.
- Dar servicio de mantenimiento en condiciones (24/7/365)
- Cumplir con los requisitos de ISO 27001
- Disponibilidad de Sistemas XXXX%
- SLA de respuesta a incidentes: XX horas desde recepción de comunicaciones en centro de contacto.
- Cumplir con requisitos PCI DSS v3.2.1 (si aplica)

Identificación de requisitos de USUARIOS FINALES

- Servicios disponibles:
  - Sistemas de apoyo ante interrupciones
  - Mantener servicios de soporte ante interrupciones
- Protección de datos: los productos y servicios protegen adecuadamente los datos de los usuarios finales cumpliendo los requisitos legales tanto para los datos de contacto como para los datos confidenciales.

Identificación de requisitos de SOCIOS

Los socios serán empresas que contratan nuestras aplicaciones para dar servicio a usuarios finales:

Comentado [4]: NOTAS sobre las partes interesadas:

Las necesidades y expectativas son solo aquellas relevantes para la seguridad de la información.
Los requisitos legales y reglamentarios así como las obligaciones contractuales pueden incluirse en los requisitos de las partes interesadas
Algo que parece evidente pero quo conviene resaltar es que Ud. necesita averiguar lo que las partes interesadas quieren de usted, y necesita averiguar cómo satisfacer todos estos requisitos en su SGSI

Comentado [5]: Agregar/eliminar los items que sean necesarios.

Deben ir en correlación con lo puesto en 6.2.2

- ➔ Cumplir con los requisitos de desarrollo de Software según los acuerdos firmados
- ➔ Cumplir con los acuerdos de confidencialidad firmados
- ➔ Proporcionar información técnica y soporte suficiente que les permita desarrollar y mejorar su Interfaz de Programación de Aplicaciones (API)
- ➔ Proporcionar la formación necesaria tanto técnica como comercial enfocada a la venta de los productos y servicios
- ➔ Cumplir los acuerdos contractuales especialmente en los tiempos de entrega acordados.

Identificación de requisitos de PROVEEDORES

- ➔ Cumplir con los acuerdos contractuales
- ➔ Cumplir con las formas de pago acordadas
- ➔ Cumplir con los acuerdos de confidencialidad firmados

Identificación de requisitos de EMPLEADOS

- ➔ Proporcionar un ambiente de trabajo seguro y apropiado.
- ➔ Recibir capacitación y apoyo requeridos.
- ➔ La compañía especifica claramente sus requisitos y expectativas de los trabajadores.
- ➔ Protección de su información personal.
- ➔ La compañía paga justamente por el trabajo.
- ➔ Continuidad del empleo
- ➔ Oportunidades para el avance y desarrollo profesional

Identificación de requisitos de ASEGURADORAS

- ➔ Cumplir con los requisitos de la política
- ➔ Fidelidad en los pagos
- ➔ Comunicación de cambios en las circunstancias del negocio y del riesgo

Identificación de requisitos de administración, legales y regulatorios

- ➔ Cumplir con políticas y procedimientos internos de la organización.
- ➔ Cumplir con los requisitos de las leyes de protección de datos.
- ➔ Identificar y cumplir con los requisitos legales propios de cada tipo de negocio emprendido
  - ◆ Ley de comercio electrónico
  - ◆ Ley general de telecomunicaciones
  - ◆ Otras
- ➔ Información mediante planes de comunicación y procedimientos establecidos para mitigar su impacto.
- ➔ Se debe implementar y operar el SGSI y/o sus equivalentes, contar con la aprobación de su documentación y producir los registros requeridos por la norma:

Comentado [6]: Estos son ejemplos, colocar los que sean pertinentes al negocio.

- ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información Requisitos.
- PCI DSS v 3.2.1
- OTRAS NORMATIVAS/REGULACIONES

7.2.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La información relacionada a los análisis internos y externos (contexto) del SGSI que intervienen y afectan al logro de sus objetivos y que fueron desarrollados en la sección **7.1.2 Contexto de SGSI**. Esta información ha sido usada para definir el alcance respecto a:

- Procesos
- Características del Negocio
- Organización
- Ubicación
- Activos
- Tecnología
- Justificación de la Exclusión

De manera similar, de la sección **7.2.2. Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas** se tomarán en cuenta los Requisitos de Seguridad de la Información que provienen de los involucrados y afectados por el SGSI para delimitar el alcance de:

- Activos
- Justificación de la Exclusión

Finalmente, las dependencias de las actividades de otras organizaciones que, como en el caso anterior, también influyen en el alcance de:

- Procesos
- Características del Negocio

.

Procesos y servicios

El SGSI Información aplica a todas las funciones, servicios, actividades y activos de información, del proceso [nombre del proceso] que es parte de la Cadena de Valor definido en el Plan Estratégico de [nombre de la institución].

Procesos y/o servicios	Área	Dependencias/Interfaces

Comentado [7]: [Especificar los servicios y/o procesos de negocios que se incluyen en el alcance]. Considerar que el SGSI suele alcanzar los procesos/servicios que otorguen valor a la organización.

Se puede mostrar el alcance forma gráfica también, mencionando los procesos alcanzados y los que no.

internos alcanzados		
Ej: “Proceso de Desarrollo”	Tecnología	
“Procesos de Operaciones de TI”		
“Proceso de Operaciones	Operaciones	

Procesos y/o servicios internos NO alcanzados	**Área**	**Justificación para la exclusión.**
Ej: proceso de compras		

Características del negocio

El negocio de **[nombreempresa]** se encuentra en la industria **[nombreindustria].** El servicio provisto es el siguiente:

- ➔ Funcionalidad y/o servicio 1
- ➔ Funcionalidad y/o servicio 2
- ➔ Funcionalidad y/o servicio 3
- ➔ Funcionalidad y/o servicio 4

Organización

nombreempresa cuenta con una estructura que presenta a los distintos órganos y las relaciones que existen entre ellos representado mediante el siguiente organigrama.

Colocar organigrama

Para un detalle más específico de las relaciones funcionales que existen se cuenta con los descriptivos de los roles y responsabilidades de la empresa-

Ubicación

Las instalaciones donde se desarrollan los procesos alcanzado corresponden a la siguiente ubicación geográfica:

- Colocar dirección y país donde se encuentra ubicado la provisión de servicios.

Activos

Los activos de información de **[nombreempresa]** dentro del alcance y límites del SGSI están sujetos al proceso de Gestión de Riesgos, por lo que estos son inventariados, clasificados y valorizados en base al procedimiento de Gestión de Riesgos vigente y pueden ser encontrados en el Inventario de Activos que se produce a partir de la ejecución del mencionado procedimiento y teniendo en cuenta los lineamientos de la Gestión de Activos y Clasificación de la Información de la Política de Seguridad de la Información.

Tecnología

Los activos se encuentran a su vez soportados por una estructura tecnológica compleja, la cual cuenta con hardware, software, infraestructura y servicios que permiten procesar, almacenar y transmitir la información del proceso. Los componentes tecnológicos más importantes son listados en en el Inventario de Activos vigente.

7.3 Liderazgo

7.3.1. Liderazgo y compromiso

Comentado [8]: Cubre 5.1 Liderazgo y compromiso de la ISO/IEC 27001

La Alta Gerencia y los miembros del Directorio de [nombreempresa] demuestran su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información mediante las siguientes acciones:

- Reconociendo y suscribiendo la Política de Seguridad de la Información y la Declaración de Objetivos de Seguridad de la Información, revisando y validando que son compatibles con la Dirección estratégica de la organización.
- Asegurando que se realice la integración de los requisitos del sistema de gestión de la información dentro de los procesos de la organización mediante la aprobación de los procedimientos y documentos requisito del SGSI.
- Garantizando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles mediante la aprobación de partidas presupuestarias que ha dispuesto consultorías para la implementación del SGSI y sus controles.
- Comunicando, mediante los canales que considere pertinente, la aceptación de las políticas y procedimientos de seguridad de la información para la adecuación de la empresa a los requisitos del SGSI.

- Garantizando que el sistema de seguridad de la información logre sus resultados esperados, mediante las revisiones periódicas del sistema.
- Dirigiendo, indicando las correcciones que deben hacerse y brindando respaldo al personal para la realización de las medidas para mejorar la efectividad del SGSI.
- Dando recomendaciones de mejora continua para el SGSI.
- Brindando apoyo mediante el respaldo a las convocatorias y los cambios requeridos para la operación y mejora del SGSI.

7.3.2. Política de Seguridad

Comentado [9]: Cumple 5.2 PSI de la ISO/IEC 27001.

La Política de Seguridad de Información de **[nombreempresa]** cuenta con las siguientes características:

- Ha sido revisada y aprobada por la Dirección para garantizar su alineamiento al propósito de la organización.
- Referencia a los Objetivos de Seguridad de la Información.
- Reconoce la necesidad de atender los requisitos aplicables a la empresa en temas de Seguridad de Información.
- Reconoce la necesidad de mejorar y corregir continuamente el SGSI mediante la aplicación de acciones de mejora continua y acciones correctivas.
- Ha sido difundida al personal de la institución mediante charlas de concientización y comunicada por INDICAR MEDIO DE COMUNICACIÓN.
- El Oficial de Seguridad de la Información una vez al año o cuando se produzca algún cambio significativo, propondrá al Comité de Gestión de Seguridad de Información la actualización de la Política de Seguridad de la Información.

Comentado [10]: O Alta Gerencia

7.3.3. Roles, responsabilidades y autoridades

Comentado [11]: Cumple 5.3 Roles, responsabilidades y autoridades en la organización de la ISO/IEC 27001.

La Dirección de **[nombreempresa]** ha suscrito el documento Roles y Responsabilidades del SGSI que establece:

- Todos los roles necesarios para llevar a cabo las actividades requeridas por el estándar ISO/IEC 27001:2013.
- Las responsabilidades que asume cada uno de los actores involucrados en el SGSI, producto de la asunción de los roles establecidos y especificados.
- La responsabilidad del Oficial de Seguridad como encargado de informar sobre el desempeño del SGSI a la Dirección y al resto del personal que se encuentre involucrado o interesado.

En ese sentido, el Plan de Comunicaciones deja evidencia de la comunicación de los resultados del desempeño del SGSI a la Dirección.

7.4 Planificación

7.4.1 Acciones para tratar los riesgos y oportunidades

[nombreempresa] planifica la Gestión de Riesgos del SGSI y oportunidades tomando como base el entendimiento obtenido **7.2 Comprender las necesidades y expectativas de las partes interesadas.** Esta gestión está orientada a:

- Identificar nuevos controles para garantizar el logro de resultados del SGSI, que se evidencia mediante las mediciones de los controles.
- Anticiparse a los riesgos para evitar o reducir efectos perniciosos, que se evidencia con el análisis, evaluación y tratamiento de riesgos.
- Constituir una fuente de robustecimiento del SGSI, apoyando a la mejora continua, que se evidencia durante la implementación de los nuevos controles que se han definido en el Plan de Tratamiento de Riesgos.

Para los riesgos y oportunidades identificados, la empresa establece:

- Las acciones para manejarlas.
- La forma en que se implementarán en los procesos mediante Plan de Tratamiento de Riesgos.
- La forma en que serán medidas en cuanto a su efectividad.

Evaluación de los riesgos de seguridad de la información

[nombreempresa] dispone de la realización de una evaluación de riesgos, que considera:

- Definir los criterios de aceptación y de evaluación de los riesgos.
- Establecer una metodología objetiva para la evaluación de los riesgos que arroje resultados consistentes.
- Identificar riesgos de seguridad de la información (asociados a pérdida de confidencialidad, integridad y disponibilidad) y sus causantes, dentro del alcance del SGSI.
- Analizar los riesgos (consecuencias del impacto, probabilidad, nivel de riesgo).
- Evaluar los riesgos, comparando los resultados del análisis con los criterios y priorizándolos.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros asociados:

- Inventario de activos de Información.
- Análisis de riesgos.
- Evaluación de riesgos.

Tratamiento de los riesgos de la seguridad de la información

[nombreempresa] establece el tratamiento de los riesgos de seguridad de la Información considerando:

- Tomar los resultados de la evaluación de riesgos para seleccionar opciones de tratamiento.
- Determinar los controles para implementar la opción seleccionada.
- Asociar los controles a los listados en el Anexo A de la norma ISO/IEC 27001:2013 y/o otras normas, legislaciones y/o regulaciones a las que esté sujeta, para verificar que no existan omisiones.
- Elaborar la Declaración de Aplicabilidad, que especifica los controles requeridos/excluidos y el sustento de su inclusión/exclusión.
- Proponer el Plan de Tratamiento de Riesgos.
- Obtener la aprobación de los poseedores de riesgos del Acta de Aceptación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros producidos como resultado del proceso:

- Plan de Tratamiento de Riesgos.
- Declaración de Aplicabilidad.
- Acta de Aceptación del Plan de Tratamiento de Riesgos y los Riesgos Residuales.

7.4.2 Objetivos de Seguridad de Información y planificación para alcanzarlos

[nombreempresa] establece sus Objetivos de Seguridad, bajo un enfoque de alto nivel, pero estrechamente relacionado a los objetivos institucionales. Estos objetivos:

Comentado [12]: La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información.

- Son consistentes con la Política de Seguridad de Información y son referenciados desde ella.
- Son relacionados directamente con las métricas del SGSI, lo cual permite a su vez medirlos.
- Sus actualizaciones toman en cuenta los resultados de los Análisis de Contexto y Requerimientos de Seguridad de las Partes Interesadas y de los resultados de ejecución de la Metodología de Gestión de Riesgos.
- Son publicadas y comunicadas conjuntamente con la Política de Seguridad de Información, según lo establece el Plan de Comunicación.
- Son actualizables, si es requerido.
- Se determina qué se hará, qué recursos se usarán, quién será el responsable y cuándo será completado el Plan de Acciones de Mejora Correctiva, Preventiva y de Mejora.
- Son medidos y obtenidos los resultados de la efectividad de lo desarrollado

7.5 Apoyo / Soporte

Comentado [13]: Cumple clausula 7

7.5.1 Recursos

[nombreempresa] elabora una vez al año el Presupuesto Anual, en el que también se consideran los recursos requeridos para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Dicho Presupuesto es aprobado por Alta Gerencia.

Asimismo, se garantiza la participación de los recursos humanos necesarios para el SGSI, mediante decisión del Comité de Gestión de Seguridad de la Información. También se cuenta con el nombramiento formal del Oficial de Seguridad de la Información.

Comentado [14]: o Alta Gerencia.

La Superintendencia dispone de los recursos de infraestructura tecnológica y física (si corresponde), que han sido establecidas en el apartado **7.2.3 Determinar el alcance del sistema de gestión de la seguridad de la información** de este documento.

7.5.2 Competencia

[nombreempresa] dispone lo siguiente:

- Ha determinado las competencias necesarias de las personas que operan y asumen funciones específicas dentro del SGSI, las cuales han sido definidas en el documento Roles y Responsabilidades del SGSI.
- Se ha asegurado el cumplimiento de estas competencias mediante la capacitación y concientización del personal, lo que se ha documentado en el Plan de Capacitación y Concientización en Seguridad.
- Este plan puede ser actualizado si se detectan deficiencias en el conocimiento del personal, de manera que se programan capacitaciones adicionales. Para identificarlas se cuenta con métricas que evalúan el know how adquirido.

7.5.3 Concientización

Las charlas de concientización realizadas son realizadas, según lo especificado en el Plan de Capacitación y Concientización de Seguridad:

- Difusión de la Política de Seguridad de Información mediante envío de dicho documento por INDICAR MEDIO DE COMUNICACIÓN a todo el personal de la empresa. Cabe resaltar que la política forma parte de los temas tratados en las charlas de sensibilización.
- Importancia de las acciones del personal para la efectividad del SGSI.
- Beneficios de las mejoras en el desempeño del SGSI.
- Las implicancias a la empresa acerca de una no conformidad sobre el SGSI.

Cada charla de capacitación y concientización programada cuenta con la Lista de Asistencia de Capacitación.

7.5.4 Comunicación

Las comunicaciones internas y externas del SGSI son planificadas y controladas mediante el Plan de Comunicaciones, documento que es actualizado conforme se avanza con la operación del sistema, éste define:

- Comunicación
- Emisor
- Destinatarios
- Fecha de emisión
- Procesos afectados
- Estado

7.5.5 Documentación de la Información

General

El SGSI cuenta con:

- Los documentos y registros que son requisito de la norma.
- Documentos que sin ser requisito de la norma son usados por **[nombreempresa]** para asegurar la efectividad del SGSI (reglamentación interna, políticas específicas de seguridad de información, documentación de controles de seguridad de información).

Creación y actualización

[nombreempresa] dispone para la creación y actualización de sus documentos del SGSI:

- La identificación y descripción del documento: título, fecha de elaboración, autor, código.
- Definición de formatos para los documentos y registros, ya sean en medio electrónico o físico.
- La especificación de quiénes elaboran, revisan y aprueban los documentos.

Control de la información documentada

La documentación del SGSI de **[nombreempresa]** es controlada y garantiza su disponibilidad e idoneidad. Adicionalmente se vela por su adecuada protección.

Esto se logra a través de la aplicación de actividades de control:

- Distribución restringida, acceso controlado, mecanismos de recuperación y restricciones de uso.
- Condiciones adecuadas de almacenamiento y conservación.
- Control de cambios sobre los documentos, retención y disposición.

7.6 Operación

Comentado [15]: Cumple clausula 8

7.6.1 Planificación y control operacional

En el punto **7.4.1 Acciones para tratar los riesgos y oportunidades** de este documento se especifican los procedimientos y actividades que se llevan a cabo para planificar, implementar y controlar el proceso de Gestión de Riesgos.

Para todos los casos indicados anteriormente se cuenta con procedimientos documentados que a su vez generan registros que son evidencia de las actividades realizadas.

7.6.2 Evaluación de los riesgos de seguridad de la información

La frecuencia y condiciones para la realización de las Gestiones de Riesgo son especificadas en el procedimiento Gestión de Riesgos del SGSI.

Los resultados de la Evaluación de Riesgos se encuentran documentados y dejan registros que evidencian su realización.

7.6.3 Tratamiento de los riesgos de seguridad de la información

La empresa propone e implementa el Plan de Tratamiento de Riesgos, según lo dispone el procedimiento Gestión de Riesgos del SGSI.

Las actividades del Tratamiento de Riesgos dejan registros que evidencian su realización.

7.7 Evaluación del desempeño

7.7.1 Monitoreo, medición, análisis y evaluación

[nombreempresa] mide y evalúa la efectividad del SGSI, para lo cual determina:

- Aquello que requiere ser monitoreado y medido: procesos y controles de la seguridad de información.
- Los métodos aplicados para monitorear, medir, analizar y evaluarlos, para obtener resultados válidos.
- Cuándo se llevarán a cabo el monitoreo y las mediciones.
- Quién es el responsable de las mediciones.
- Cuándo se analizarán y evaluarán los resultados del monitoreo y de las mediciones.
- Quién es el responsable del análisis y evaluación de los resultados.

7.7.2. Auditorías internas

[nombreempresa] lleva a cabo a intervalos planificados auditorías internas para determinar que el SGSI:

- Cumpla con los requerimientos de su SGSI y con los lineamientos del estándar ISO/IEC 27001:2013. Contempla, adicionalmente, otras regulaciones y/o normativas que la empresa esté sujeta.
- Se encuentra implementado y se mantiene de manera efectiva.

Ambos puntos son realizados según se dispone en el Plan de Auditoría Interna De igual forma, la empresa estable que:

- Planifica, establece, implementa y mantiene un programa o programas de auditoría (frecuencia, métodos, responsabilidades, requisitos de planificación y reporte) tomando en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas.
- Define los criterios y alcance de la auditoría en el Plan de Auditoría Interna.
- Selecciona auditores objetivos e imparciales.
- Comunica los resultados de las auditorías a los jefes involucrados y Alta Gerencia dejando registro de ello en el Plan de Comunicaciones.
- Se mantienen registros que evidencian la planificación y ejecución de la Auditoría en el:
  - Programa Anual de Auditoría Interna
  - Plan de Auditoría Interna
  - Cronograma de Auditoría Interna Acta de Reunión de
  - Auditoría Interna
  - Informe de Auditoría Interna

7.7.3 Revisión por parte de la Dirección

La Alta Gerencia y los miembros del Directorio que conforman a [nombreempresa] realizan una revisión anual del SGSI para garantizar su disponibilidad, adecuación y efectividad. Esta revisión comprende:

Comentado [16]: Puede ser el Comité de SI también.

- El estado de las acciones generadas por revisiones de la Dirección previas.
- Cambios significativos internos y externos, relevantes para el SGSI.
- El desempeño de la Seguridad de Información en la empresa::
  - No conformidades y acciones correctivas.
  - Resultados de métricas e indicadores.
  - Resultados de auditoría.
  - Grado de cumplimiento de los objetivos del SGSI.
- Retroalimentación de las partes interesadas.
- Los resultados de la Gestión de Riesgos del SGSI y el estado del Plan de Tratamiento de Riesgos.

- ➔ Oportunidades de Mejora Continua.

Todos estos elementos son preparados y presentados a la Dirección mediante Informes y los resultados de la revisión conllevan a la emisión de acciones correctivas y de mejora.

Producto de la revisión, se cuenta con evidencias documentadas de su realización en el Acta de Revisión por la Dirección, donde se indican los resultados y acciones definidas durante la misma.

Comentado [17]: Puede ser le Comite de SI también.

7.8 Mejora

7.8.1 No conformidad y acción correctiva

Al presentarse una no conformidad, la empresa dispone:

- ➔ Reaccionar frente a la misma, disponiendo la acción para controlarla, corregirla y atender las consecuencias de ésta.
- ➔ Considerar si es necesario y posible eliminar la causa de la no conformidad, mediante: su revisión, determinación de las causas de la no conformidad y verificación de no conformidades similares.
- ➔ Implementar las acciones planeadas.
- ➔ Revisar la efectividad de las acciones realizadas.
- ➔ Realizar cambios sobre el SGSI, si es requerido.

El manejo de estas condiciones para las acciones correctivas se encuentra especificado en el procedimiento Acciones Correctivas del SGSI. Estas acciones son acordes y proporcionales a las no conformidades que las originaron.

Asimismo, se mantiene registro de las correcciones realizadas.

7.8.2 Mejora continua

Para realizar acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSI, **[nombreempresa]** establece los lineamientos de Mejora Continua del SGSI mencionados anteriormente.

8.
Versionado

Confeccionado por:	MEDIREC
Código de documento:	CÓDIGO DE DOCUMENTO
Versión:	NUM DE VERSION 1
Fecha última de actualización:	18/07/24
Revisado por:	MEDIREC
Aprobado por:	MEDIREC