POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código	PO-GGN-001 (Rev 2)	**Fecha de Creación**	18/02/2023
Proceso	POLI: Gestión de Políticas	**Fecha de Aprobación**	05/08/2024
Área	GGN: Gerencia General	**Fecha Vigencia**	05/08/2024
Aprobador	Alan Weschler		
Norma y Referencia	ISO/IEC 27001:2013 6.1 Acciones para tratar los riesgos y oportunidades		

1. Objeto, Alcance y Usuarios

El propósito de esta política es:

a) Definir el marco de referencia de VIGATEC para la protección de la confidencialidad, la integridad y la disponibilidad de la información de la organización y de terceros.
b) Establecer directrices, en relación con la gestión de la seguridad de la información según lo establecido en la norma ISO/IEC 27001.
c) Minimizar los riesgos que amenazan a los activos de información que gestiona la organización.
d) Implementar y fomentar una cultura de Seguridad de la Información al interior de VIGATEC y con terceros con los que se relaciona.

El alcance de esta Política se encuentra acotada a lo definido en el Campo de Aplicación del Manual Sistema de Gestión de Seguridad de la Información.

Esta Política es aplicable a colaboradores de VIGATEC, es decir, a los empleados, a los proveedores de servicios y subcontratistas.

2. Descripción de esta Política

2.1 Objetivos de la Seguridad de la Información

Para la definición de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), se deben realizar las siguientes actividades:

a) Identificación de las tareas esenciales que se deben realizar.

b) Identificación los activos de información y los recursos claves.

c) Determinación de responsables.

d) Establecimiento de un período para el cumplimiento de los objetivos.

e) Establecimiento de un criterio de evaluación de los resultados.

Cada uno de estos puntos debe ser evaluado a partir de los resultados del análisis de riesgos que se genera anualmente. En el proceso de determinación de estos objetivos y de los registros respectivos, es necesario tomar en cuenta los requerimientos aplicables de la seguridad de la información, siendo estos consistentes con la presente Política. Una vez establecidos los objetivos, estos deben ser gestionados para dar cumplimiento de sus metas. Dicho documento tiene periodicidad anual y es representativo de los objetivos de la seguridad de la información requeridos por el SGSI.

Los objetivos determinados para el período deben ser comunicados a toda la organización en el alcance. La comunicación se debe realizar a través de correo electrónico u otro medio que la organización considere apropiado.

2.2 Gestión de los Riesgos

Conocer el impacto que los riesgos de la seguridad de la información tienen sobre la organización a raíz de las amenazas y vulnerabilidades en las que operan los distintos sistemas de información, es una actividad fundamental para identificar los incidentes que pueden ocurrir en la organización, ya que nos permite definir acciones más adecuadas para su tratamiento.

La organización debe implementar una metodología que permita crear un proceso de evaluación de riesgos, de acuerdo con lo siguiente:

a) Definir cómo identificar los riesgos que podrían causar la pérdida de confidencialidad, integridad o disponibilidad de la información de la organización.
b) Definir cómo identificar a los dueños del riesgo.
c) Definir criterios para evaluar las consecuencias del riesgo y su probabilidad de ocurrencia.
d) Definir cómo se calcula el riesgo.
e) Definir el criterio de aceptación de riesgos.

La evaluación de riesgos da lugar a la generación de un plan de tratamiento de riesgos.

2.3 Comité de Seguridad de la Información

Con el objeto de asegurar el cumplimiento de esta Política General de Seguridad de la Información, VIGATEC ha establecido una Estructura Organizacional de Seguridad de la Información que contempla la definición de funciones específicas en el ámbito de la seguridad.

VIGATEC ha conformado el Comité de Seguridad de la Información, el cual se debe encargar de desarrollar, implementar y realizar seguimiento a todas las iniciativas e incidentes que se relacionen con la Seguridad de la Información, en especial la Política

General de Seguridad de la Información, sus ajustes y modificaciones, el cual está conformado por personal de la alta administración de la empresa, conforme a su Estatuto.

Las funciones del Comité se describen en su Estatuto Comité Seguridad de la Información (ES-GGN-001), de las cuales caben destacar las siguientes:

a) Aprobar las Políticas de Seguridad.
b) Definir el Sistema de Gestión de Seguridad de la Información.
c) Solicitar auditorías, diagnóstico y seguimiento de las políticas y del Sistema de Gestión de Seguridad de la Información.
d) Hacer seguimiento de los incidentes de seguridad de la información.
e) Solicitar que se regule el tratamiento de la información desde el punto de vista de la seguridad de algún recurso o proceso que no lo tuviese.
f) Asegurar el entrenamiento y capacitación en prácticas de seguridad de la información.

2.4 Documentos de Políticas

El presente documento constituye una política de alto nivel, destinada a documentar la definición de los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo. Complementando la presente política, VIAGTEC ha desarrollado las políticas de seguridad que determinó necesarias para regular, con mayor grado de detalle, los recursos de información de acuerdo con las disposiciones mencionadas en esta Política General.

La alta dirección de VIGATEC es responsable por la presente Política General de Seguridad de la Información, quien debe asegurar que sea de conocimiento de todos los colaboradores.

La presente Política y las demás complementarias, son disponibilizadas en la aplicación ISOEASY, de manera que cada empleado incluido en el alcance del SGSI, pueda acceder a ella, desde la inducción que se realiza al ingresar a la organización o al cambiarse de área a una incluida en el alcance del SGSI. Las políticas que se consideran necesarias disponibilizar para partes interesadas se incluyen en la página Web institucional.

Todas las políticas generadas a partir del establecimiento del Sistema de Gestión de Seguridad de la Información deben tener un respectivo dueño correspondiente a su área de injerencia, y quienes son responsables de revisar, implementar y actualizar cada documento.

Las Políticas de Seguridad de la Información deben ser revisadas anualmente por el Comité de Seguridad de la Información y sus cambios deben ser validados por el Gerente General.

2.5 De la Clasificación de la Información

La información que se maneja en VIGATEC tiene diferentes niveles de importancia en cuanto al riesgo que representa su eventual divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario clasificar la información según el nivel de daño que se genera si se compromete su confidencialidad, integridad o disponibilidad.

El propietario de la información es responsable de su clasificación y de definir las personas que tendrán acceso a ella, debiendo periódicamente revisar la clasificación determinada, con el propósito de mantenerla o modificarla según se estime apropiado.

2.6 De la Información de Clientes y Proveedores

VIGATEC, tiene información de sus colaboradores, clientes y proveedores, la cual es considerada información valiosa, por ende, se compromete a tratarlos dando pleno cumplimiento a la normativa legal y la política de tratamiento de datos personales.

2.7 De Empresas Externas y Consultores

Las empresas externas y consultores que presten servicios deben cumplir con las políticas, normas y procedimientos de seguridad de los activos de información de VIGATEC.

2.8 De las Auditorías

Con el fin de asegurar el correcto uso de los recursos de su propiedad, VIGATEC se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

2.9 Del Compromiso de VIGATEC

Con el fin de mantener el nivel de seguridad adecuado, la alta dirección se debe asegurar de:

a) Establecer, implementar, mantener y continuamente mejorar el Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos de la norma internacional ISO/IEC 27001 vigente.
b) Utilizar los recursos adecuados y que estén a su alcance para proteger sus recursos de información y capacitar a sus empleados en materias de seguridad de la información.
c) Cumplir la legislación vigente, respecto de la manipulación y resguardo de la información y materias afines, así como también de los acuerdos alcanzados contractualmente con otras empresas y empleados.
d) Adoptar el nivel de seguridad que cumpla estándares internacionales, que garanticen un tratamiento integral en la administración de la seguridad de los recursos de información, tanto al interior de la empresa como en sus comunicaciones con el exterior.
e) Definir un estándar mínimo de seguridad a todos los recursos de información.

f) Aplicar niveles de seguridad a los recursos de información, proporcionales a su criticidad y riesgo.
g) Generar los procedimientos adecuados para que el acceso a la información sea realizado sólo por usuarios debidamente autorizados, acreditados y autenticados, de acuerdo con los privilegios de acceso asignados para el desempeño de sus funciones sobre la base de su descripción de cargo.
h) Evaluar todos los proyectos relacionados con recursos informáticos de VIGATEC, desde la perspectiva de la Seguridad de la Información y a través de las áreas correspondientes.
i) Proveer los recursos necesarios para gestionar de forma adecuada los requerimientos de la política de seguridad de la información para el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.
j) Garantizar la continuidad de los procesos de negocio, mediante la implementación de planes de contingencia adecuados.
k) Realizar y mantener respaldos periódicos de la información y de los sistemas de acuerdo con su criticidad, requerimientos legales y de continuidad de negocio.
l) Definir responsables de la administración de todo recurso informático, incluyendo los aspectos relacionados con su generación, procesamiento, almacenamiento y transmisión.
m) Definir los procedimientos para que cualquier elemento que le sea entregado o retirado a un usuario cumpla con las formalidades definidas, permitiendo además mantener un registro actualizado de los equipos y software de la empresa.
n) Aplicar las sanciones correspondientes, ante la detección de actividades ilícitas o reñidas con disposiciones internas y/o que caigan dentro de lo penado por la Ley, sin perjuicio de iniciar las acciones civiles legales que la Ley le confiera.
o) Mantener estricto resguardo de la documentación o evidencia generada a partir de las actividades de seguimiento, revisión y evaluación del sistema de gestión de seguridad de la información.

2.10 De las Responsabilidades y Deberes de los Usuarios

Los Usuarios de los recursos de VIGATEC tienen las siguientes responsabilidades y deberes:

a) Mantener debida reserva y bajo resguardo la información a la cual tuviese acceso autorizado.
b) Abstenerse de acceder sin autorización escrita o indebidamente a terminales, archivos, documentación o datos de VIGATEC y clientes.
c) Abstenerse de instalar software o conectar equipos personales u otros elementos no autorizados, a la red de datos.

d) Asegurar el resguardo de la confidencialidad, integridad y disponibilidad de la información de VIGATEC y dar aviso al CISO de cualquier situación o circunstancia que pueda afectar o poner en riesgo la información o los sistemas de procesamiento de información.
e) Abstenerse de realizar actos contrarios a la propiedad física e intelectual de VIGATEC, particularmente a la incluida en entornos digitales, tales como diseños de procesos, modelos de bases de datos y aplicaciones de negocios; así como también de vulnerar contratos de licenciamiento de software y similares, suscritos por VIGATEC con sus proveedores de tecnologías de información.
f) Utilizar los recursos informáticos para desempeñar las funciones que le fueron asignadas.
g) Mantener en adecuadas condiciones los elementos de tecnología de información entregados para el desempeño de su trabajo. Conocer y cumplir las normas y procedimientos asociadas al uso de los recursos tecnológicos y activos de información a los que se le otorgue acceso, como, por ejemplo, aquellas asociadas al uso de contraseñas, del correo electrónico y del acceso a redes públicas como Internet.
h) Colaborar con los controles y procesos de auditoría orientados a verificar el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

2.11 De la Comunicación

VIGATEC debe asegurar la existencia de un proceso que permita determinar de forma clara y planificada los requerimientos de comunicación de la información relevante para la seguridad de la información, hacia todos los participantes que contribuyen al funcionamiento del SGSI, esto con el fin de que la información definida para un período determinado sea presentada por los responsables a través de los canales dispuestos para ello.

2.12 De las Competencias y Concientización en Seguridad de la Información

La Subgerencia de Personas, debe determinar las competencias necesarias del personal que pueden afectar el funcionamiento del Sistema de Gestión de Seguridad de la Información, incluyendo los siguientes elementos:

a) Se deben establecer los mecanismos adecuados para evaluar y asegurar que el personal posee la educación, capacitación o experiencia necesarios y con esto establecer las acciones correspondientes para la capacitación del personal u otra medida que la organización considere apropiada. Para tal efecto, la organización provee un proceso de entrenamiento en seguridad de la

información y procura su reedición anual en base a la retroalimentación del propio Sistema de Gestión de Seguridad de la Información.

b) Asegurar competencias en seguridad de la información a partir de los programas de entrenamiento establecidos.
c) El Comité de Seguridad de la Información debe evaluar de forma anual la efectividad de la capacitación en seguridad de la información, y a partir de esto tomar las acciones pertinentes.
d) Gestionar toda la información documentada respecto de la efectividad y rendimiento de la capacitación en seguridad de la información.
e) Dentro de los programas de capacitación, la organización vela por que todos sus empleados estén conscientes de los siguientes puntos:

- La presente Política General de Seguridad de la Información.
- La contribución que los mismos colaboradores realizan para la efectividad del Sistema de Gestión de Seguridad de la Información, incluyendo los beneficios de la mejora continua de la seguridad de la información.
- Las implicancias de no cumplir con los requerimientos del Sistema de Gestión de Seguridad de la Información.

2.13 Evaluación del Desempeño del SGSI

Para la evaluación del desempeño del SGSI, se aplica lo siguiente:

a) La alta dirección debe asegurar, la asignación de responsables, planificación y desarrollo de actividades que permitan evaluar el desempeño de funcionamiento del SGSI, con el fin de asegurar la adecuación y eficacia de este para el cumplimiento de los objetivos de seguridad de la información.
b) El seguimiento, medición, revisión y evaluación de la documentación se debe realizar en intervalos establecidos sobre los aspectos relevantes a la seguridad de la información que la organización requiera. Se debe considerar un marco de determinación de los temas a evaluar que incluya el alcance, métodos, responsables, períodos, etc.
c) Así mismo, se establece que la organización debe ser capaz de realizar auditorías internas para evaluar que el SGSI se encuentra gestionado de acuerdo con lo conformado por VIGATEC y los requerimientos de la Norma Internacional ISO/IEC 27001 vigente.
d) VIGATEC se compromete a reconocer cuales son las oportunidades de mejora continua y las actualizaciones necesarias para los diferentes aspectos del SGSI. Para tal efecto, la alta gerencia debe dar prioridad al control y revisión de los resultados de la evaluación del desempeño del SGSI.

3. Principales Responsabilidades

a) El Gerente General debe:

a. Asegurar el establecimiento de esta Política, así como de los objetivos que de ella se desprendan, y que éstos sean implementados y mantenidos.

b. Asegurar que la gestión de riesgos y oportunidades sea apropiada al propósito y contexto de VIGATEC y que apoye su dirección estratégica.

c. Asegurar que esta Política proporcione un marco de referencia para establecer los objetivos e indicadores de la gestión del riesgo.

d. Dotar de las competencias y recursos suficientes a la organización para una adecuada gestión de riesgos.

e. Aprobar la definición del alcance, el contexto y los criterios de la gestión de riesgos.

f. Aprobar el listado de riesgos inherentes y el plan de tratamiento de riesgos, que deben estar visados por el Propietario del Proceso.

g. Promover activamente en la organización una cultura de la gestión de riesgos y oportunidades, donde cada responsable de procesos conozca sus riesgos y oportunidades y adopte las acciones de mitigación o potenciación, las medidas de control correspondientes.

h. Promover una cultura preventiva en la organización, que estimule la notificación oportuna de las desviaciones o potenciales desviaciones y favorezca la corrección de los factores de riesgo que los motivaron.

i. Debe revisar al menos una vez al año esta Política, revisión que debe ser aprobada por el mismo Gerente General.

j. Proponer al Directorio para su aprobación:

- El marco de referencia de la gestión de riesgos y oportunidades.
- El nivel máximo de riesgo (apetito al riesgo) y su respectivo nivel de desviación que VIGATEC esté dispuesto a tolerar (tolerancia al riesgo).

k. Informar al Directorio y los ejecutivos de la empresa, por sí mismo o por quién éste designe, de los riesgos asociados a la seguridad de la información, y resolver respecto de las medidas de mitigación a implementar.

b) El Comité de Seguridad de la Información debe:

a. Asegurar la implementación de esta política, para lo cual le corresponde hacer seguimiento de la gestión de riesgos y oportunidades en cada sesión.

b. Proponer la metodología de gestión de riesgos y oportunidades y asegurarse de su implementación, lo que incluye:

- Proponer la definición del marco de referencia, la comunicación y consulta, que permita identificar los riesgos y oportunidades, analizarlos, valorarlos, realizar su tratamiento, seguimiento, revisión, así como el registro e informe.
- Asegurar que cada proceso cuente con un Propietario del Proceso, que cada Riesgo cuente con un Propietario del Riesgo y que cada Activo de Información, cuente con un Propietario del Activo de Información.
- Coordinar el trabajo de levantamiento, actualización y valorización de los riesgos y oportunidades de VIGATEC.
- Apoyar y controlar a los Propietarios de los Procesos, de los Riesgos y de los Activos de Información, en las tareas de mitigación y gestión de los riesgos.
- Verificar la aprobación del Riesgo Inherente y Residual por cada Propietario de Proceso, Riesgo o Activo, para ser presentado al Gerente General quien aprueba el documento final.

c. Dar visibilidad a la gestión de riesgos a las partes interesadas pertinentes del interior de la organización.

c) El Propietario del Proceso, del Riesgo o del Activo de Información, debe:

a. Asumir la responsabilidad primera de asegurar la aplicación y seguimiento de las distintas políticas y procedimientos definidos por VIGATEC para el logro de los objetivos de cada proceso.
b. Conocer los riesgos asociados a sus procesos y/o activos de la información, definir planes de mitigación y procurar la implementación de estos.
c. Conocer las oportunidades asociadas a sus procesos y/o activos de la información, definir planes de potenciación y procurar la implementación de estos.
d. Planificar sus procesos, los objetivos e indicadores, de forma coherente con esta Política, de forma de minimizar riesgos, potenciar las oportunidades, verificar desempeño y optimizar los resultados de la organización en su conjunto.
e. Aprobar la identificación del riesgo y oportunidades, el análisis, su valoración y el tratamiento aplicado.

d) Auditores calificados, deben llevar auditorías independientes, al menos una vez al año, para determinar el nivel de eficacia de la gestión de la seguridad

de la información de VIGATEC, el cumplimiento de esta Política, las normas y procedimientos definidos.

e) El Usuario VIGATEC o el Usuario Externo, debe:

a. Dar cumplimiento a los lineamientos establecidos en esta Política.
b. Reportar incidentes de seguridad de la información.

4. Publicación, Sensibilización y Capacitación

a) El Gerente General de VIGATEC debe asegurar los mecanismos para que todas las políticas, en especial la presente y sus futuras modificaciones sean conocidas y estén a disposición permanentemente por todos los directores, ejecutivos y colaboradores y sean dadas a conocer a las partes interesadas pertinentes, inclusive los proveedores, en el contexto de los servicios que le sean prestados a VIGATEC.
b) El Gerente General de VIGATEC reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en las materias indicadas en la presente Política.
c) Los ejecutivos de VIGATEC deben crear mecanismos para que esta política y sus procedimientos, sean conocidos y considerados permanentemente por todos los integrantes de la organización, asegurándose que los colaboradores asumen y comprenden sus responsabilidades. Estas acciones estarán contenidas en las actividades de capacitación anual al personal de VIGATEC.
d) Los ejecutivos de VIGATEC deben asegurar que todos los colaboradores, dentro del alcance del SGSI, cuenten con una inducción y sean capacitados en materias de esta política, manteniendo un canal de comunicación formal para informar a toda la organización respecto a los avances, logros y novedades en la materia, con el objetivo de crear una cultura de seguridad de la información dentro de la Organización.

5. Incumplimiento y Sanciones

a) Ante la ocurrencia de algún incumplimiento a las medidas orientadas a resguardar la presente Política, el usuario que lo detecte debe informar a la brevedad a su jefatura directa y/o al CISO, quienes analizarán el incumplimiento y deben gestionar las medidas necesarias para minimizar los potenciales daños a la organización y lograr el cumplimiento integral de esta política, evitando que se reiteren situaciones similares.
b) Todo colaborador tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar lo dispuesto en la presente Política. Dicha notificación se debe registrar conforme al Procedimiento Gestión de Incidentes, No Conformidades y Acciones Correctivas (PR-GGN-004).

c) Los incumplimientos graves, es decir, aquellos que afecten a los clientes, y/o a los clientes de los clientes, y/o que se manifiesten como quejas del cliente, deben ser informados al Gerente General y este debe informarlos al Directorio de VIGATEC.
d) Al colaborador que contravenga lo indicado en esta Política y/o los documentos relacionados a la misma, se le debe aplicar lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad (RE-PER-001), en cuanto a sanciones y multas (ver TÍTULO XXI).
e) Con relación al personal externo y/o proveedores que no cumplan con lo indicado en esta Política, dependiendo del tipo de incumplimiento se debe amonestar o rescindir el contrato.

6. Contexto Normativo

a) Esta Política debe responder al requisito 5.2 - Política de la norma internacional ISO/IEC 27001 vigente.
b) Esta Política, los procedimientos y demás documentos complementarios, deben mantener coherencia con los procesos, los objetivos, indicadores y los requerimientos del negocio.
c) Esta Política debe ser complementada con las demás políticas de VIGATEC.

7. Documentos Relacionados

- Política Gestión de Riesgos y Oportunidades (PO-GGN-002)
- Política Gestión de Incidentes, No Conformidades y Acciones Correctivas (PO-GGN-003)
- Política Gestión de Cambios (PO-GGN-004)
- Política Gestión de Recursos Humanos (PO-GGN-005)
- Política Capacitación (PO-PER-001)
- Política Desarrollo Seguro (PO-CIS-001)
- Política Seguridad de Proveedores (PO-CIS-002)
- Política Clasificación de la Información (PO-CIS-003)
- Política Control de Acceso (PO-CIS-004)
- Política de Pantalla y Escritorio Limpio (PO-CIS-005)
- Política Uso Aceptable de Activos (PO-CIS-006)
- Política Dispositivos Móviles y Teletrabajo (PO-CIS-007)
- Política Respaldo de Información (PO-CIS-008)
- Política Transferencia de Información (PO-CIS-009)
- Política Continuidad de Negocio (PO-CIS-011)
- Política Tratamiento de Datos Personales (PO-CIS-012)
- Política de Eliminación y Destrucción (PO-CIS-013)
- Política de Cookies (PO-CIS-014)

- Política Uso de Controles Criptográficos (PO-CIS-015)
- Política de Cumplimiento (PO-CIS-016)
- Estatuto Comité Seguridad de la Información (ES-GGN-001)
- Manual Sistema de Gestión de Seguridad de la Información (MA-GGN-001)
- Procedimiento Gestión de Incidentes, No Conformidades y Acciones Correctivas (PR-GGN-004)
- Reglamento Interno de Orden, Higiene y Seguridad (RE-PER-001)

Revisado por	Aprobado por
Víctor Iván Ocaranza Ojeda Víctor Ocaranza O. Gerente de Tecnología	 Alan Weschler R. Gerente General