Política Gestión de Riesgos y Oportunidades

Norma(s) que Aplican	Refer.Normativa	Area Proceso	Código
ISO/IEC 27001:2013	6.1 Acciones para tratar los riesgos y oportunidades	**GGN: Gerencia General**	**PO-GGN-002**
ISO/IEC 27001:2022	6.1 Acciones para tratar los riesgos y oportunidades	**POLI: Gestión de Políticas**	

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alan Weschler	**18-02-2023**	**26-04-2023**	**26-04-2023**	**2**	**04-04-2022**

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
CISO	**Gerente de Soluciones Digitales**	**(no aplica)**	**Gerente de Soluciones Digitales**	**Público**

1. Objeto, Alcance y Usuarios

El propósito de esta política es proporcionar los lineamientos y el marco de referencia que permitan a VIGATEC gestionar sus riesgos y oportunidades a que se enfrenta, en forma integrada, organizada y continua en toda la organización incluida en el alcance del SGSI.

El propósito de esta política es:

a) Definir el marco de referencia de VIGATEC para la gestión de sus riesgos y oportunidades, en forma integrada, organizada y continua.

b) Minimizar los riesgos que amenazan a los activos de información que gestiona la organización.

c) Implementar y fomentar una cultura de gestión de riesgos y oportunidades 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

a) VIGATEC integra a sus actividades operacionales y su sistema de gestión, la gestión de riesgos y oportunidades por considerar que es un requerimiento del negocio y una herramienta efectiva para aplicar acciones proactivas.

b) VIGATEC ha determinado que la gestión de riesgos y oportunidades debe considerar todos los procesos de la organización, incluidos en el alcance del SGSI, especialmente aquellos considerados críticos para el resultado del negocio.

c) VIGATEC pone énfasis en la necesidad de sincronizar el adecuado conocimiento de los riesgos y

oportunidades con el diseño de las estrategias de negocio y la definición y desarrollo de las metas necesarias para su logro, considerando los riesgos y oportunidades observados y las prioridades definidas según el grado de tolerancia de riesgo definido por el Gerente General.

d) La totalidad de las áreas de VIGATEC incluidas en el alcance del SGSI, y sus ejecutivos y colaboradores deben contribuir a generar soluciones frente a los distintos riesgos y potenciar oportunidades que se presenten o detecten en la operatoria diaria, proponiendo acciones mitigadoras para dichos riesgos y acciones potenciadoras para las oportunidades.

e) VIGATEC debe informar con transparencia a las partes interesadas pertinentes sobre los niveles de riesgo de la empresa, las medidas adoptadas y los avances para su control, manteniendo los canales adecuados para favorecer la comunicación.

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 y oportunidades.

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

f. Una vez que cada Propietario de Proceso aprueba sus riesgos y/u oportunidades inherentes, con las propuestas de tratamiento y eventuales riesgos residuales, los cuales tienen el prisma propio del Propietario del Proceso, el Comité de Seguridad de la Información debe verificar la consistencia de la identificación, análisis, valoración y propuesta de tratamiento, para que el Gerente General finalmente, apruebe el tratamiento del riesgo y/u oportunidad residual, no sólo para el Propietario del Proceso, sino para la organización en su conjunto. Con ello, se pueden poner en implementación los tratamientos correspondientes.

g. Promover activamente en la organización, incluida en el alcance del SGSI, 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, incluida en el alcance del SGSI, 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 si 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 6.1 - Acciones para tratar los riesgos y oportunidades 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 General Seguridad de la Información (PO-GGN-001)
- 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)
- Política Uso de Software de Código Abierto (PO-CIS-017)
- Estatuto Comité Seguridad de la Información (ES-GGN-001)
- Manual Sistema de Gestión de Seguridad de la Información (MA-GGN-001)
- Procedimiento Gestión de Riesgos y Oportunidades (PR-GGN-003)
- Procedimiento Gestión de Incidentes, No Conformidades y Acciones Correctivas (PR-GGN-004)
- Declaración de Aplicabilidad (SoA) (RE-CIS-001)
- Reglamento Interno de Orden, Higiene y Seguridad (RE-PER-001)