VIGATEC
Innovación · Compromiso · Experiencia

Manual de Gestión

Política Gestión de Recursos Humanos

Norma(s) que Aplican	Refer.Normativa	Area Proceso	Código
ISO/IEC 27001:2013	A.7 Seguridad relativa a los recursos humanos	GGN: Gerencia General	PO-GGN-005

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Andrés Loyola	25-05-2022	03-06-2022	03-06-2022	1	25-05-2022

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Subgerente de Personas	Gerente General	(no aplica)	Subgerente de Personas	Público

1. Objetivo

El propósito de esta política es definir los lineamientos que permitan asegurar que los colaboradores del SGSI de VIGATEC, entiendan sus responsabilidades y que se realicen las actividades de contratación adecuadas para las funciones requeridas por el negocio.

2. Alcance

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.

3. De Carácter General

3.1 Antes del Empleo

3.1.1 Investigación de Antecedentes

a) Para el personal considerado en la contratación para actividades incluidas en el SGSI de VIGATEC se debe realizar la revisión de los antecedentes curriculares, con el fin de verificar el cumplimiento de los requisitos definidos para el puesto y asegurar la contratación de personas idóneas de acuerdo con los requisitos y objetivos de cumplimiento de la seguridad de la información.

La verificación de antecedentes se realizará solicitando lo siguiente:

- Revisión de Curriculum vitae
- Solicitud de Certificado de título, estudio o especialización post grado
- Solicitud de Certificado de antecedentes: Sólo para personal crítico que accede a información secreta.
- Cualquier otro documento de interés de acuerdo con tipo y condiciones de la contratación.

b) En los casos que sea posible, la información obtenida debe ser verificada para confirmar la veracidad de dichos datos a través del contacto con las fuentes que corresponda.

c) Todos los candidatos deben pasar por una entrevista técnica que valida los conocimientos y competencias específicas requeridas para el puesto (realizada por la jefatura directa) y por una entrevista psicolaboral que evalúa las habilidades blandas, motivación y capacidad de adaptación a la cultura organizacional (realizada por psicólogos de la Subgerencia de Personas).

d) La organización debe asegurar que el tratamiento de los candidatos y la información obtenida durante el proceso de contratación cumpla fielmente las disposiciones de la ley de protección y privacidad de la información de carácter personal y cualquier otra normativa legal que corresponda.

3.1.2 Términos y Condiciones del Empleo

a) Para formalizar la contratación de un candidato, se deben considerar los siguientes aspectos:

- Firma del Contrato de Trabajo, además de Acuerdo de Confidencialidad y No Revelación de la Información relativa a su cargo y al negocio.
- Entregar la Política General de Seguridad de Información y los aspectos relevantes (básicos) del funcionamiento del SGSI, tales como derechos de acceso, clasificación de la información y manejo de la misma.
- Informar las responsabilidades y roles para la seguridad de la información relativas al cargo o servicio contratado.
- Informar las responsabilidades que la organización establece en caso de término de la relación contractual.

b) Los requisitos establecidos anteriormente deben ser aceptados en su totalidad por parte del candidato contratado como parte de sus condiciones de contratación.

c) La definición de responsabilidades posteriores al término de contrato, deben ser consideradas a nivel general de la organización teniendo en cuenta los requisitos legales, de seguridad de la información, de confidencialidad y/o de secretos industriales, sin embargo estos pueden ser revisados caso a caso, ya que pueden variar dependiendo de las condiciones o acuerdos de las partes.

3.2 Durante el Empleo

3.2.1 Responsabilidades de Gestión

a) Para el personal del SGSI, VIGATEC debe constantemente hacer hincapié en el compromiso

requerido por parte de los usuarios para el resguardo de la seguridad de la información, reforzando las funciones y responsabilidades individuales y los requerimientos y directrices definidos en la Política General de Seguridad de la Información. Para ello debe disponer de canales de comunicación adecuados para lograr una ejecución correcta de estrategias de concientización en la materia.

b) Se debe reforzar además el requisito fundamental de que los usuarios comuniquen los incidentes de seguridad que identifiquen.

c) Para el personal del SGSI, VIGATEC puede considerar la medición del apego a la normativa relativa al resguardo de la seguridad de la información, a través de pruebas o testeos generales de conocimiento, así como también de conocimiento relativo a los requerimientos del cargo.

3.2.2 Concienciación, Educación y Capacitación en Seguridad de la Información

Con la finalidad de que los usuarios del SGSI de VIGATEC estén conscientes de sus responsabilidades para la seguridad de la información, se debe establecer un plan de capacitación anual que establezca actividades de entrenamiento, capacitación y concientización que esté alineado con las políticas y procedimientos asociados al SGSI.

El plan de capacitación debe considerar lo siguiente:

- La comunicación del compromiso que el Gerente General entrega al resguardo de la seguridad de la información y las actividades relacionadas.
- Conocimiento de las obligaciones normativas del SGSI y las normativas legales y regulatorias en el contexto del alcance del SGSI.
- Responsabilidades individuales relativas a la Seguridad de la Información.
- Los procedimientos de Gestión de Incidentes de Seguridad de la Información.
- Los resultados y análisis de las mediciones relativas al funcionamiento del SGSI.

3.2.3 Proceso Disciplinario

En caso de existir brechas de seguridad asociadas a incumplimientos de un usuario a las normativas establecidas en la Política General de Seguridad de la Información y cualquier otra normativa asociada al SGSI, la organización dispone del Reglamento Interno de Orden, Higiene y Seguridad, el cual contiene las definiciones relativas a procesos disciplinarios y la forma en que se deben aplicar.

3.3 Finalización del Empleo o Cambio en el Puesto de Trabajo

3.3.1 Responsabilidades Ante la Finalización o Cambio de Contrato

a) Para toda ocasión en que una relación contractual termina, la VIGATEC debe realizar un catastro de los acuerdos que siguen vigentes de forma posterior al término de dicho contrato. Dicha información debe ser comunicada a las partes de acuerdo con los términos definidos en PO - Procedimiento de Selección, Contratación y Desvinculación (PR-PER-002)

b) En caso de requerimientos de cambios contractuales se deben tener las mismas consideraciones establecidas en el punto 3.3.1.a.

4. De Gobierno

Respecto de esta Política las responsabilidades de los principales roles, son las que se describen a continuación:

a) El Gerente General debe:

   a. Asegurar el establecimiento de esta Política.

   b. Dotar de las competencias y recursos humanos calificados a la organización para una adecuada implementación del SGSI.

   c. Verificar que el Comité de Seguridad de la Información revisa al menos anualmente esta Política, revisión que debe ser aprobada por el mismo Gerente General.

   d. Informar al Directorio y los ejecutivos de la empresa, por si mismo o por quién éste designe, de los incidentes de seguridad de la información que comprometan esta Política.

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 incidentes, no conformidades y acciones correctivas en cada sesión.

   b. Proponer la metodología de gestión de incidentes, no conformidades y acciones correctivas.

   c. Dar visibilidad a la gestión de capacitación al interior de la organización, conforme al alcance del SGSI.

c) Cada Gerente, 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 incidentes, no conformidades y acciones correctivas asociados a sus procesos y/o activos de la información, definir planes de acción y procurar la implementación de estos, sin demora.

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.

5. Contexto Normativo

a) Esta Política debe cumplir los requerimientos 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.

6. Publicación

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.

7. Sensibilización y Capacitación

a) El Gerente General de VIGATEC reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en las materias indicadas en la presente Política.

b) 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.

c) 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.

8. Incumplimiento

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.

9. Sanciones

a) 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).

b) 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.

10. Documentos Relacionados

- Política General Seguridad de la Información (PO-GGN-001)
- Política Gestión de Riesgos y Oportunidades (PO-GGN-002)
- Política Gestión de Incidentes, No Conformidades y Acciones Correctivas (PO-GGN-003)
- Estatuto Comité Seguridad de la Información (ES-GGN-001)
- Manual Sistema de Gestión de Seguridad de la Información (MA-GGN-001)
- PO - Procedimiento de Selección, Contratación y Desvinculación (PR-PER-002)
- Procedimiento Gestión de Incidentes, No Conformidades y Acciones Correctivas (PR-GGN-004)
- Reglamento Interno de Orden, Higiene y Seguridad (RE-PER-001)

Documentos Relacionados por Enlaces (8)

Comentarios (3)

Enlaces hacia este Documento (1)