VIGATEC
Innovación · Compromiso · Experiencia

Manual de Gestión

Política Uso de Controles Criptográficos

Norma(s) que Aplican	Refer.Normativa	Area Proceso	Código
ISO/IEC 27001:2013	A.10.1 Controles criptográficos	**CIS: CISO - Sistema de Gestión de Seguridad de la Información**	**PO-CIS-015**

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Andrés Loyola	**17-05-2022**	**03-06-2022**	**03-06-2022**	**1**	**17-05-2022**

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
CISO	Gerente General	Jefe de Informática y Procesos	Gerente de Soluciones Digitales	Uso Interno

1. Objetivo

El propósito de esta Política es establecer los lineamientos para asegurar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información en las operaciones del SGSI de VIGATEC.

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

a. Se debe hacer uso de técnicas criptográficas para los activos de información que tengan nivel de clasificación de información "**Secreto**" y que se encuentren afectos al procesamiento de las siguientes actividades:

   a. Acceso físico o lógico de cualquier índole.

   b. Transmisión de información a través de correo electrónico u otros medios de comunicación.

c. Almacenamiento en medios de soporte electrónico.

d. Almacenamiento o procesamiento desde dispositivos móviles.

b. Todo propietario de un activo de información que tenga nivel de clasificación "**Secreto**", debe realizar una evaluación de riesgos que se concentre en las debilidades y amenazas a las que se somete el activo de información frente al uso actual de métodos criptográficos. En base a los resultados de la evaluación, el Propietario de Activo debe realizar una propuesta de control mediante uso de técnicas criptográficas para el resguardo del activo de información en cuestión.

c. Para tal efecto, el Propietario del Activo debe considerar objetivos de seguridad basados en los siguientes criterios:

a. Confidencialidad: Uso de cifrado de información para protección de información, tanto para el almacenamiento como la transmisión.

b. Integridad o Autenticidad: Uso de firmas electrónicas para la verificación de la integridad de la información o la autenticidad de la misma en el almacenamiento y en la transmisión.

c. No repudio: Uso de técnicas criptográficas que permitan evidenciar la existencia de un evento o de una acción.

d. Autenticación: Uso de técnicas criptográficas que permitan autenticar usuarios (colaboradores) y otras entidades del sistema que soliciten acceso a, o transacciones con, usuarios, entidades y recursos del sistema.

d. El uso de técnicas criptográficas propuesto por el Propietario del Activo de información, debe ser aprobado por el CISO.

e. La información involucrada en los servicios de aplicaciones que pasan a través de redes públicas se debe proteger contra actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada, considerando controles criptográficos para:

- Fortalecer el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte (por ejemplo, por medio de autenticación con certificado digital).
- Procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales claves.
- Determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, por ejemplo, asociados con procesos de ofertas y contratos.
- El nivel de confianza requerido en la integridad de los documentos clave.

f. El Jefe de Informática y Procesos, es responsable por la gestión de las claves, de forma tal que se

asegure la protección y el uso adecuado y seguro de claves criptográficas a través de todo su ciclo de vida, es decir:

- Generación de claves criptográficas privadas y públicas.
- Activación y distribución de claves criptográficas.
- Definición del plazo para el uso de las claves y de su actualización periódica (de acuerdo con la evaluación de riesgos).
- Archivo de claves inactivas que son necesarias para archivos electrónicos encriptados.
- Destrucción de claves.

g. Las claves son administradas por sus propietarios, en conformidad con las reglas indicadas precedentemente.

h. El Jefe de Informática y Procesos, es responsable de la administración y operación del sistema de gestión de claves.

i. El Jefe de Informática y Procesos, es responsable que se elaboren y apliquen apliquen procedimientos para la gestión segura de claves secretas y privadas, así como también para la validación de autenticidad de las claves públicas.

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 por el establecimiento de esta Política y su adecuación a los procesos y al negocio.
   b. Verificar que el Comité Seguridad de la Información revise al menos una vez al año la presente política, revisión que debe ser aprobada por el mismo Gerente General.
   c. Informar al Directorio de los incidentes del SGSI de VIGATEC.

b) El Comité Seguridad de la Información debe:
   a. Informar al Gerente General y a la plana ejecutiva, de los riesgos asociados al uso de áreas seguras y resolver respecto de las medidas de mitigación a implementar.
   b. Verificar que los eventos e incidentes han sido registrados, asignar un responsable del análisis e implementación y hacer seguimiento hasta verificar la eficacia de la acción tomada.
   c. Revisar la presente Política, al menos una vez al año.

c) Cada Gerente, Jefatura de Área y Propietario de Proceso, debe:
   a. Permanentemente aplicar y resguardar el fiel cumplimiento de la presente política y los documentos relacionados.

b. Asegurarse de que los incidentes sean registrados, analizados y se implementen acciones correctivas o de mejora, de forma de evitar la recurrencia.

d) 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)
- Procedimiento Gestión de Incidentes, No Conformidades y Acciones Correctivas (PR-GGN-004)
- Reglamento Interno de Orden, Higiene y Seguridad (RE-PER-001)

Fin del documento.
Copia no controlada si se imprime. Consultar última versión vigente en sistema documental.
Cualquier modificación, copia o fotocopia a este documento queda totalmente PROHIBIDA.

Documentos Relacionados por Enlaces (7)
Comentarios (8)
Enlaces hacia este Documento (1)