Prestador de Servicios de Certificación

PS01
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INFORMACIÓN DEL DOCUMENTO

NOMBRE	PS01 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
REALIZADO POR	THOMAS SIGNE
PAÍS	CHILE
VERSIÓN	1.4
Fecha	JUNIO DE 2023
TIPO DE DOCUMENTO	PÚBLICO
CÓDIGO	THS-CL-AC-POL-02
REQUISITO	PS01

Historial de versiones

VERSIÓN	**FECHA**	**DESCRIPCIÓN**
1.0	02/04/2019	ELABORACIÓN DE DOCUMENTO INICIAL.
1.1	23/07/2021	CAMBIO DE NOMBRE DE DOCUMENTO. SE HACE REFERENCIA EXPLÍCITA A LAS POLÍTICAS QUE COMPONEN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. MENCIÓN EXPLÍCITA AL CUMPLIMIENTO DE ISO 27001 A.5
1.2	16/09/2021	Cambio de imagen THS Ajuste al formato de documento vigente
1.3	18/01/2022	Revisión anual de políticas. Inclusión del apartado 6.
1.4	12/06/2023	Revisión del apartado 6. Inclusión del apartado 7.

ÍNDICE

1 OBJETIVO 4
2 ALCANCE 4
3 DOCUMENTACIÓN RELACIONADA 4
4 DEFINICIONES Y ABREVIACIONES 4
4.1 ACRÓNIMOS Y ABREVIACIONES 4
4.2 DEFINICIONES 4
5 ACTIVIDADES 7
5.1 CUMPLIMIENTO DEL REQUERIMIENTO NORMATIVO 7
5.1.1 REQUERIMIENTOS NORMATIVOS CUBIERTOS 7
5.1.2 REQUERIMIENTOS SOPORTADOS DE LA GUÍA DE ACREDITACIÓN 7
5.2 DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 7
5.3 COMPROMISO DE LA ALTA DIRECCIÓN 8
5.4 DOCUMENTOS RELACIONADOS 9
6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 10
6.1 RIESGOS 10
6.2 ACTUALIZAR POLÍTICA Y NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN 11
6.3 DIFUSIÓN DE LA POLÍTICA Y NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN 11
6.4 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 12
6.5 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS 13
6.6 GESTIÓN DE ACTIVOS 13
6.7 CONTROL DE ACCESO 14
6.8 CRIPTOGRAFÍA 14
6.9 SEGURIDAD FÍSICA Y DEL ENTORNO 14
6.10 SEGURIDAD DE LAS OPERACIONES 15
6.11 SEGURIDAD DE LAS COMUNICACIONES 15
6.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 16
6.13 RELACIÓN CON PROVEEDORES 16
6.14 GESTIÓN DE INCIDENTES 16
6.15 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 17
6.16 CUMPLIMIENTO 17
6.17 COMITÉ DE SISTEMAS DE GESTIÓN 17
6.18 RELACIÓN ENTRE EL PLAN DE SEGURIDAD Y LOS RECURSOS ASIGNADOS 18
7 TRAZABILIDAD ENTRE ISO 27002-POLÍTICA DE SEGURIDAD-DPC-PC 18
7.1 RELACIÓN DEL PLAN DE SEGURIDAD CON LAS PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN 18
8 FORMATOS 18
9 REGISTROS 18

1 OBJETIVO

El objeto de esta política es definir la sistemática mediante la cual Thomas Signe, gestiona las políticas asociadas al sistema de gestión de seguridad de la información, para la administración de sus servicios como Autoridad de Certificación, en el marco del cumplimiento de la Guía de Acreditación del Organismo de Acreditación competente.

2 ALCANCE

Estos lineamientos son de aplicación a las políticas de seguridad de la información requeridas por la norma ISO 27.001 y aquellas otras que entienda Thomas Signe como requeridas para el cumplimiento de sus DPC y PC. Esta política es de cumplimiento obligatorio por Thomas Signe y aplicable a todos los servicios de certificación brindados por Thomas Signe.

3 DOCUMENTACIÓN RELACIONADA

Esta política se complementa y adhiere a lo indicado en el documento GSIGNE-SI-PR-05 políticas de seguridad de la información.

4 DEFINICIONES Y ABREVIACIONES

4.1 ACRÓNIMOS Y ABREVIACIONES

PSC PRESTADOR DE SERVICIOS DE CERTIFICACIÓN
PKI INFRAESTRUCTURA DE LLAVE PÚBLICA
AR AUTORIDAD DE REGISTRO
DPC DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
PC POLÍTICA DE CERTIFICACIÓN
CRL LISTA DE CERTIFICADOS REVOCADOS
OCSP ONLINE CERTIFICATE STATUS PROTOCOL
DSCF DISPOSITIVOS SEGUROS DE CREACIÓN DE FIRMA
CPS Certification Practices Statements

4.2 DEFINICIONES

Algoritmo: conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Autoridad de Certificación: Certification Authority (CA). Es una entidad de confianza, responsable de emitir y revocar los certificados digitales, publicación de certificados, publicación de listas de certificados revocados, etc. Nombrada dentro de la normativa chilena como Prestador de Servicios de Certificación– PSC.

Autoridad de Registro: Persona jurídica, con excepción de los notarios públicos, o parte interna de los PSC necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para: Registrar las peticiones que hagan los solicitantes para obtener un certificado; y comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones. Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

Autoridad de sellado de tiempo (TSA): entidad de confianza que emite sellos de tiempo mediante una o más TSU. Nombrada dentro de la normativa chilena como Prestador de Servicios de Certificación– PSC. Los sellos de tiempo emitidos por la PSC, conforme a la regulación establecida por la AUTORIDAD ACREDITADORA, incluyen la fecha y hora referenciada por la fuente de tiempo reportada por el Servicio Hidrográfico y Oceanográfico de la Armada de Chile.

CA Raíz: Autoridad de Certificación de primer nivel, base de confianza.

CA subordinada: Autoridad certificadora de segundo nivel o más niveles.

Certificado digital: mensaje de datos electrónico firmado por la PSC, el cual identifica tanto a la PSC que lo expide, como al suscriptor y contiene la clave pública de este último.

Clave privada: ver Datos de Creación de Firma.

Clave pública: ver Datos de Verificación de Firma.

Cliente: en los servicios de certificación digital, él término "cliente" identifica a la persona natural o jurídico con la cual la PSC establece una relación comercial.

Datos de Creación de Firma (Clave privada): valores numéricos únicos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

Datos de Verificación de Firma (Clave pública): datos que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor.

Declaración de Prácticas de Certificación (DPC): documento en el que constan de manera detallada los procedimientos que aplica la PSC para la prestación de sus servicios. Una declaración de las prácticas que la PSC emplea para emitir sellos de tiempo.

Prestador de Servicios de Certificación: entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada (Ley N°19.799 artículo 1°, letra c).

Sellado de tiempo (o Time stamping en inglés): mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

Firma Digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Función Hash: operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Log: servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

Niveles de seguridad: diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

OID: identificador único de objeto (object identifier). OID. Acrónimo del término en idioma inglés "Object Identifier", que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

PKI: Infraestructura de clave pública (Public Key Infraestructure). Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que solo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.
- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

Proveedor: el término "proveedor" incluye a organizaciones, personas, fabricantes, distribuidores, ensambladores de tecnología y otros que suministran productos, bienes y servicios. Entre los proveedores de las PSC están: Entidades recíprocas, empresas de tecnología que prestan servicios en sus diferentes modalidades como son: hosting, colocación, repositorio documental (electrónico o físico), proveedor de dispositivos, proveedor de telecomunicaciones, etc.

Revocación: proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación, al presentarse alguna de las causas establecidas en la Declaración de Prácticas de Certificación para la emisión de certificados.

Servicio de certificación digital: conjunto de actividades certificación que ofrece la PSC para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

Solicitante: persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una PSC, demuestra el cumplimiento de los requisitos establecidos en la DPC para acceder al servicio de certificación digital. Persona natural que solicita a la PSC el servicio de sello de tiempo (la emisión de sellos de tiempo).

Titular: persona natural o jurídica que, habiendo firmado el respectivo Contrato de Prestación de Servicios o de Suscripción, acepta las condiciones del servicio de sello de tiempo prestado por la PSC.

Tercero que confía (Tercero aceptante): persona natural o jurídica que recibe un documento, log, notificación o cualquier otro dato, firmado digitalmente o no, con un sello de tiempo emitido por la PSC, y que confía en la validez de dicho sello de tiempo.

Unidad de sellado de tiempo (TSU): conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo.

5 ACTIVIDADES

5.1 CUMPLIMIENTO DEL REQUERIMIENTO NORMATIVO

La Política de Seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridadque son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por Thomas Signe. Si Thomas Signe externaliza en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

Esta Política de Seguridad tiene las siguientes características:

- Los objetivos de seguridad son consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal quelos objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que Thomas Signe sea un ente de confianza.
- Está basada en las recomendaciones del estándar ISO 27002 sección 5.
- Es lo suficientemente general para permitir alternativas de implementación tecnológica.
- Dada la complejidad de los objetivos, la política está conformada por más de un documento.

5.1.1 REQUERIMIENTOS NORMATIVOS CUBIERTOS

Este documento y los documentos relacionados buscan cubrir los siguientes requerimientos normativos

Guía de Evaluación Procedimiento de Acreditación PSC FEA. Requisito PS02.
LEY N°19.799, ARTÍCULO 14. y 15.
REGLAMENTO, Art. 22 y. 23, REGLAMENTO DISPOSICIÓN TRANSITORIA PRIMERA, SEGUNDA Y TERCERA.
ISO/IEC 9594-8
ITU-T X.690 5.
ISO27001
Políticas para la seguridad de la información
Revisión de las políticas para la seguridad de la información

5.1.2 REQUERIMIENTOS SOPORTADOS DE LA GUÍA DE ACREDITACIÓN

En la estructura presentada se soportan los requerimientos del numeral 4.8.2 de la Guía de Acreditación de FEA.

5.2 DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En Thomas Signe de Chile S.A, somos conscientes de la importancia de ofrecer la mejor calidad de nuestros productos y servicios. Asumimos nuestra responsabilidad en el mantenimiento de los niveles de calidad y de seguridad de la información necesarios para generar la confianza de nuestros clientes.
Forma parte de la Política Estratégica de Thomas Signe de Chile S.A. el desarrollo y la implantación de un sistema de gestión de integrado de seguridad de la información y requisitos de las Guías de Evaluación para el Procedimiento de Acreditación del Ministerio de Economía, Fomento y Turismo del Gobierno de Chile basado en el análisis, la prevención y la mejora continua, aportando para ello la Alta Dirección los recursos necesarios para su consecución.
En Thomas Signe de Chile S.A. hemos incorporado los principios y directrices, que a continuación exponemos:

- La orientación de nuestros esfuerzos va dirigida a la prevención de errores, en vez de a su control y corrección.
- La calidad de nuestros productos y servicios constituye una ventaja competitiva frente a otros competidores y contribuye a mantener y a mejorar nuestra posición en el mercado.
- La promoción, en nuestras relaciones comerciales con nuestros proveedores y partes interesadas, de los mismos principios de seguridad de la información que aplicamos.
- La participación de todos es clave para conseguir los objetivos establecidos por Thomas Signe de Chile. lo que redundará en el bien de nuestros clientes.
- La formación continua y la concienciación del personal es un elemento básico.
- Asegurar que la empresa cumple con los requisitos de nuestros clientes además de con los requisitos legales y reglamentarios aplicables, haciendo especial foco en aquellos establecidos en la legislación en materia de seguridad de la información.
- Establecer acciones sistemáticas de control, monitorización y prevención de incidentes
- Garantizar la confidencialidad, integridad y disponibilidad de la información protegiendo los datos y los sistemas contra accesos indebidos y actualizaciones no autorizadas.
- Establecer acciones sistemáticas de control, monitorización y prevención de incidentes.
- Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos.
- Esta Política se pone a disposición del público en nuestra página web https://www.thomas-signe.cl/.

THOMAS SIGNE opera como prestador de servicios de certificación (PSC). La Autoridad de Certificación Subordinada "THOMAS SIGNE CHILE" emite certificados digitales a personas naturales personas jurídicas y personas vinculadas a

empresas, conforme a lo establecido en la Ley N°19.799 sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma.

THOMAS SIGNE forma parte de la Jerarquía de Certificación de THOMAS SIGNE ROOT, que está compuesta por una Autoridad de Certificación Raíz y varias Autoridades de Certificación Subordinadas entre las que se encuentra "THOMAS SIGNE CHILE Autoridad de Certificación"

Para llevar a cabo la prestación de los servicios de certificación, THOMAS SIGNE subcontrata la infraestructura tecnológica y recursos humanos a la Empresa del Grupo SIGNE, según permite la Ley N°19.799. No obstante, los servicios subcontratados se llevan a cabo según lo establecido en la Declaración de Prácticas y Políticas de Certificación de THOMAS SIGNE y en los acuerdos suscritos entre SIGNE y THOMAS SIGNE.

La Dirección de Thomas Signe es responsable de establecer y mantener los controles efectivos sobre las operaciones y procedimientos, incluyendo las Manifestaciones de sus prácticas de negocio como AC, la integridad del servicio (incluyendo controles para gestionar el ciclo de vida de las claves, los certificados, los dispositivos criptográficos, en este último caso, si procede) y los controles del entorno de las AC. Estos controles contienen mecanismos de monitorización y se toman acciones para corregir las deficiencias encontradas.

Existen limitaciones inherentes en algunos controles, incluyendo la posibilidad de errores humanos y la evasión o anulación de los controles. En las ocasiones en que un análisis de riesgos recomienda la inclusión de controles compensatorios para cubrir las mencionadas limitaciones inherentes, éstos se incluyen. Aun así, incluso los controles efectivos pueden proporcionar solamente una seguridad razonable en relación con las operaciones, procedimientos y entorno de Thomas Signe como PSC. Adicionalmente, debido a cambios en las condiciones, la efectividad de los controles puede variar cada cierto tiempo.
Por todo ello, THOMAS SIGNE en colaboración con SIGNE, y con pleno apoyo de la dirección, se compromete a lo siguiente:

- Hacer públicas sus Prácticas de Negocio sobre la gestión del ciclo de vida de las claves, los certificados, así como su política de privacidad de la información y proporciona sus servicios conforme a dichas afirmaciones.
- Mantiene controles efectivos para proporcionar una seguridad razonable de que:
    - La información del suscriptor es autenticada correctamente (para las actividades de registro realizadas por THOMAS SIGNE)
    - La integridad de claves, certificados gestionados se mantiene a lo largo de todo su ciclo de vida
    - La privacidad de las claves privadas se mantiene a lo largo de todo su ciclo de vida
    - El acceso a la información de suscriptores y usuarios está restringida a personal autorizado y la información está protegida de usos no especificados en las prácticas de negocio publicadas por THOMAS SIGNE
    - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las clavesy los certificados
    - Las tareas de explotación, desarrollo y mantenimiento de los sistemas de la AC sonadecuadamente autorizadas y realizadas para mantener la integridad de los mismos

Todo ello alineado con los estándares internacionalmente aceptados:

- ISO 27001 Information Technology – Security techniques – Information security management systems – Requirements.
- ISO 27002 Tecnología de la información – Técnicas de Seguridad – Código de Prácticas para los controles de seguridad de la información.
- WEBTRUST (SM/TM) FOR CERTIFICATION AUTHORITIES, Trust Service Principles and Criteria for Certification Authorities.

5.3 COMPROMISO DE LA ALTA DIRECCIÓN

La Gerencia General es consciente de la importancia del cumplimiento de la Política del Sistema de Gestión en todas las actividades de certificación digital, para garantizar que los servicios sean entregados de acuerdo a los requisitos del sistema de gestión, normativos, legales y del cliente.

PRINCIPIO 1: DECLARACIÓN DE PRÁCTICAS DE NEGOCIO
Declaración de Prácticas y Políticas de Certificación para "THOMAS SIGNE" (www.thomas-signe.cl), incluyendo:

- Declaración de Prácticas de Certificación para Firma Electrónica Avanzada
- Política de Certificación de Firma Electrónica Avanzada de Persona Natural
- Política de Certificación de Firma Electrónica Avanzada de Pertenencia a Empresa
- Política de Certificación de Firma Electrónica Avanzada de Persona Jurídica

PRINCIPIO 2: INTEGRIDAD DEL SERVICIO

- Controles de la Gestión del Ciclo de Vida de las Claves
- Generación de las claves de la AC
- Almacenamiento, copias de seguridad y recuperación de las claves de la AC
- Distribución de la clave pública
- Uso de las claves de la AC y de los certificados de entidad final
- Destrucción de las claves de la AC
- Archivo de claves de AC
- Gestión del ciclo de vida de hardware criptográfico
- Servicio de Gestión de la provisión de la clave del suscriptor
- Controles de la Gestión del Ciclo de Vida de los certificados
- Registro de suscriptores
- Emisión de certificados
- Revocación de certificados
- Distribución de certificados
- Información sobre el estado de los certificados
- Gestión del ciclo de vida del DSCF

PRINCIPIO 3: CONTROLES AMBIENTALES DE LA AUTORIDAD DE CERTIFICACIÓN

- Restringir el acceso lógico y físico a los sistemas de CA y los datos dando solo acceso a las personas autorizadas
- Mantener la continuidad de las operaciones de gestión de claves, certificados
- Autorizar y ejecutar adecuadamente la operación, el mantenimiento y el desarrollo de los sistemas de la Autoridad de Certificación, con el fin de mantener su integridad.

5.4 DOCUMENTOS RELACIONADOS

Políticas	**Documento que la desarrolla**	**A quién se comunica**
Política general de seguridad de la información	Política de sistemas de gestión	Empleados Proveedores de servicio Clientes
Control de acceso	GSIGNE-SI-PR-09 Control de acceso GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Clasificación de la información	GSIGNE-SI-PR-08 Gestión de activos GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Seguridad física y ambiental	GSIGNE-SI-PR-11 Seguridad física y del entorno	Personal con responsabilidades en el SGSI
Uso adecuado de los activos	GSIGNE-SI-PR-07 Gestión de activos GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Puesto de trabajo despejado y pantalla limpia	GSIGNE-GRAL-PR-08 Políticas internas	Empleados
Transferencia de información	GSIGNE-SI-PR-13 Seguridad de las comunicaciones GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Dispositivos móviles y teletrabajo	GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Restricciones de instalación y uso del software	GSIGNE-GRAL-PR-08 Políticas internas	Empleados Proveedores de servicio
Copias de seguridad	GSIGNE-SI-PR-12 Seguridad de las operaciones	Área de SI
Protección ante el software malicioso	GSIGNE-SI-PR-12 Seguridad de las operaciones	Área de SI Empleados

Gestión de vulnerabilidades técnicas	GSIGNE-SI-PR-12 Seguridad de las operaciones	Área de SI
Controles criptográficos	GSIGNE-SI-PR-10 Criptografía	Área de SI Empleados
Seguridad de las comunicaciones	GSIGNE-SI-PR-13 Seguridad de las comunicaciones	Área de SI

6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación se describen los documentos que implementan el plan de gestión de seguridad de la información el cual corresponde a un Sistema de Gestión de Seguridad de la Información acreditado bajo la norma ISO27001, donde el documento "GSIGNE-GRAL-MSG Manual de Sistemas de Gestión" describe las cláusulas 4 a 10 de la norma ISO 27001 y el documento "THS-CL-SI-PR-01 Gestión del riesgo - 00 SoA" indica los procedimientos y políticas que en base al análisis y gestión de riesgos cubren los requerimientos del anexo A de la norma ISO27001 que cubre los siguientes objetivos de Control y controles:

GSIGNE-SI-PR-01 Gestión del riesgo
GSIGNE-SI-PR-05 Políticas de Seguridad de la Información
GSIGNE-SI-PR-06 Organización de la seguridad de la información
GSIGNE-SI-PR-07 Seguridad relativa a los recursos humanos
GSIGNE-SI-PR-08 Gestión de activos
GSIGNE-SI-PR-09 Control de acceso
GSIGNE-SI-PR-10 Criptografía
GSIGNE-SI-PR-11 Seguridad fisica y del entorno
GSIGNE-SI-PR-12 Seguridad de las Operaciones
GSIGNE-SI-PR-13 Seguridad de las comunicaciones
GSIGNE-SI-PR-14 Adquisicion, desarrollo y mantenimiento
GSIGNE-SI-PR-15 Relación con proveedores
GSIGNE-SI-PR-16 Gestión de incidentes
GSIGNE-SI-PR-17 Aspectos SI para la GCN
GSIGNE-SI-PR-18 Cumplimiento

Nota: todos los documentos están referenciados y relacionados con los controles en el documento "THS-CL-SI-PR-01 Gestión del riesgo - 00 SoA".

6.1 RIESGOS

La organización 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 dispone de un procedimiento de Gestión del Riesgo- Metodología, en el que se describen los siguientes puntos:

- Metodología de análisis de Riesgo
  - Identificación de Activos
  - Tipos de Activos
  - Valoración de Activos
  - Valoración de Amenazad
  - Salvaguardas
  - Impacto
    - Impacto acumulado
    - Impacto repercutido
  - Cálculo del riesgo
  - Niveles de riesgo aceptable y residual
    - Riesgo aceptable
    - Riesgo residual
    - Responsabilidades
- Plan director de seguridad
  - Acciones/Procesos del Plan director de Seguridad
  - Verificación del Plan director de Seguridad
  - Seguimiento
- Análisis de impacto en el negocio
  - Introducción

- Alcance y propósito
- Fases
  - Identificación de los procesos de negocio
  - Escalones de interrupción
  - Impacto de la interrupción
  - Prioridades de la recuperación
  - Recursos necesarios

El proceso de Gestión de Riesgos en la Organización se realiza de acuerdo con las siguientes actividades:

- Identificación de activos
- Criterios de valoración
- Cálculo del riesgo
- Determinación del riesgo aceptable
- Declaración de Aplicabilidad (SoA)

El desarrollo de estas actividades se encuentra recogido en el procedimiento GSIGNE-SI-PR-01 Gestión del Riesgo.

Una vez determinado el nivel de riesgo aceptable por la organización se procederá a la elaboración de un Plan director de seguridad que recoge los requisitos del Plan de Tratamiento de Riesgos según ISO 27001.

Los criterios de valoración definidos en la organización serán objeto de revisión y se podrá realizar la modificación de los mismos para adecuar los niveles de seguridad a las necesidades del momento.

Así mismo, la Dirección de la organización definirá un nivel de riesgo aceptable apoyado en los mismos criterios de valoración que se han utilizado en la metodología.

Obtenido el valor del riesgo de los diferentes activos se hará la evaluación del mismo comparando los valores obtenidos con el nivel aceptable marcado. En todos aquellos activos cuyo valor de riesgo esté por encima del aceptable, deberá ser tratado para reducirlo hasta un nivel aceptable o bien, ser asumido mediante decisión explícita de los responsables de la organización.

En la gestión de la seguridad de la información, las medidas de seguridad a aplicar, (denominadas también salvaguardas o controles), se seleccionarán de las definidas en el Anexo A del estándar UNE-ISO/IEC 27001.

6.2 ACTUALIZAR POLÍTICA Y NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Según lo establecido en el documento GSIGNE-SI-PR-05 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, apartado 5.1.2 revisión de las políticas para la seguridad de la información.

Tanto la Política de Seguridad de la información es revisada periódicamente, o cuando los procesos de revisiones detecten cambios importantes en los recursos tecnológicos, operacionales o en el ambiente de negocios de Thomas Signe que pudiesen afectar el contenido y alcance de la Política y/o Normativa. Este proceso de revisión será coordinado y gestionado por el Oficial de Seguridad de la Información.

El conjunto de todas las políticas se revisa anualmente en el proceso de revisión por la dirección. Además, en caso de ser requerido por cambios en los sistemas, se pueden actualizar las políticas cuando se considere necesario.

Las políticas serán aprobadas a nivel del Comité de Sistemas de Gestión y aquellas para las que sea requerida se pasarán a la firma.

Siempre que se realicen cambios en las políticas, y al menos una vez al año, se deberán de difundir a los todos miembros de la organización.

6.3 DIFUSIÓN DE LA POLÍTICA Y NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

La Política, prácticas de seguridad y Normativa de Seguridad de la Información son difundidas al personal de Thomas Signe a través de los medios utilizados por el Grupo Signe según el punto 7.4 del Manual de Sistemas de Gestión, GSIGNE-GRAL-MSG Manual de Sistemas de Gestión, que indica lo siguiente:

Los medios utilizados para asegurar la comunicación interna y externa eficaz son:

- Páginas web de las empresas.
- Redes sociales
- Correo electrónico.
- Tablones de anuncios.

- Comunicación personal directa.
- Reuniones
- NEWS
- Softwares internos
- Gestor documental

Y más en concreto:

CONTENIDO	CUANDO	A QUIÉN	QUIÉN DEBE COMUNICAR	MEDIO
Funciones y responsabilidades	Continuo	Empleados	RRHH	Varios (Email, softwares internos)
Políticas internas	Continuo y cuando se produzcan cambios	Empleados	RSG	Varios (email, intranet, gestor documental)
Política de los Sistemas de Gestión	Continuo y cuando se produzcan cambios	Empleados y terceros	RSG	Varios (web, email, intranet, gestor documental)
Procedimientos del sistema de gestión	Continuo	Empleados	RSG	Gestor documental
Información Comercial	A criterio de Departamento de Marketing	Clientes	Departamento de Marketing	Varios (email, llamadas, etc.)
Información pública	Continuo	Público en general	Departamento de Marketing	Varios (web, redes sociales)
Información interna	Continuo	Empleados	RRHH – Departamento de Marketing	Varios (web, email, gestor documental)
Información a proveedores	Continuo	Proveedores	RSG – Dirección Operaciones (Compras)	Varios (Web, email).
Información a clientes	Continuo	Clientes	Dirección Comercial	Comunicados
Información sobre incidentes de SI a partes interesadas	Incidencias de SI que lo requieran	Partes interesadas	Dirección de Sistemas de Información	Email

6.4 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Compromiso de las organizacional con la seguridad de la información:

- La organización debe velar por que sus procesos cumplan con lo establecido en esta normativa y participar en los procesos periódicos de evaluación de riesgo de seguridad de la información que defina.
- Las evaluaciones de riesgo de seguridad de la información que se realicen deben considerar activos como aplicaciones e infraestructura, así como proceso de seguridad de la información utilizados por servicios externalizados que soportan las operaciones del Thomas Signe.
- La priorización y frecuencia de las revisiones de la evaluación de riesgo de seguridad de la información sobre activos deben basarse, siempre que sea posible, en los niveles de riesgo identificados en procesos de evaluación anteriores o de estadísticas de incidentes de seguridad de la información. La descripción de la evaluación de riesgo de seguridad de la información para los diferentes activos aparece en la Metodología de Gestión de Riesgo Tecnológico.
- Las deficiencias detectadas como resultado de una evaluación de riesgos de seguridad de la información y los correspondientes planes de acción que sean requeridos deben cumplir con un proceso de seguimiento hasta su cierre.
- Las deficiencias, problemas o incidentes relacionados a los procesos de tecnología deben satisfacer los requisitos técnicos y de gestión con un enfoque de riesgo.

- Las excepciones a las normas de seguridad de la información detectadas durante los procesos de los puntos 5 y 6 deben cumplir con los requisitos definidos en cada caso.

Según el documento interno GSIGNE-SI-PR-06 Organización de la Seguridad de la información se describen los procedimientos a seguir en materia de las siguientes actividades:

- Organización Interna
  - Roles y responsabilidades en seguridad de la información.
  - Segregación de tareas
  - Contactos con las autoridades
  - Contactos con grupos de interés especial
  - Seguridad de la información en gestión de proyectos
- Dispositivos móviles
  - Política de dispositivos móviles
  - Teletrabajo

6.5 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

La seguridad relativa a los recursos humanos define la sistemática mediante la que el Grupo Signe y por ende Thomas Signe, gestiona los aspectos relacionados con la seguridad relativa a los recursos humanos y es desarrollado en el documento "GSIGNE-SI-PR-07 Seguridad relativa a los recursos humanos", cuyo ámbito de aplicación es a los requisitos relativos a la seguridad asociada a los recursos humanos (tanto internos como externos) requeridos por la norma ISO 27.001. Aplica a las distintas empresas incluidas dentro del alcance de los sistemas de gestión de seguridad de la información. Incluye también los siguientes documentos:

GSIGNE-PR-RRHH-02 Selección de Personal
THS-CL-AC-RRHH-01 PE01 Procedimiento de Seguridad del Personal ACG
GSIGNE-PR-RRHH-01 Funciones y Responsabilidades
THS-CL-RRHH-PR-01 Funciones y Responsabilidades
THS-CL-AC-MO-01 Diagrama Organizacional
GSIGNE-PR-RRHH-05 Procedimiento Sancionador
GSIGNE-PR-RRHH-03 Formación

Según este documento interno, se describen los procedimientos a seguir en materia de seguridad en los recursos humanos:

- Antes del empleo
  - Investigación de antecedentes
  - Términos y condiciones del empleo
- Durante el empleo
  - Responsabilidades de Gestión
  - Concienciación, educación y capacitación en seguridad de la información
  - Proceso disciplinario
- Finalización del empleo o cambio en el puesto de trabajo
  - Responsabilidades ante la finalización o cambio

6.6 GESTIÓN DE ACTIVOS

La sistemática seguida por Thomas Signe como parte del Grupo Signe para la identificación de los activos de información y asegurar que la información recibe el nivel adecuado de protección de acuerdo con su importancia para el Grupo Signe, se encuentra desarrollada en el procedimiento Gestión de Activos, documento "GSIGNE-SI-PR-08 Gestión de activos"

En este documento se describen los procesos de:

- Responsabilidad sobre los activos
  - Inventario de activos
  - Propiedad de los activos
  - Uso aceptable de los activos
  - Devolución de los activos
- Clasificación de la información
  - Clasificación de la información
  - Etiquetado de la información
  - Manipulación de la Información
- Manipulación de los soportes

- Gestión de soportes extraíbles
- Eliminación de los soportes
- Soportes físicos en tránsito
- Custodia

6.7 CONTROL DE ACCESO

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de control de acceso asociados al dominio 09 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-09 Control de acceso
GSIGNE-PR-GRAL-08 Políticas internas

En el documento interno GSIGNE-SI-PR-09 Control de acceso, se describen los procesos de:

- Requisitos del negocio para el control de acceso.
  - Políticas de control de acceso
  - Acceso a las redes y a los servicios de red
- Control de acceso de los usuarios
  - Registro y baja de un usuario
  - Gestión de privilegios de acceso
  - Gestión de la información secreta de autenticación de los usuarios
  - Revisión de los derechos de acceso de los usuarios
  - Retirada o reasignación de los derechos de acceso
- Responsabilidades del usuario
  - Uso de la información secreta de autenticación
- Control de acceso a sistemas y aplicaciones
  - Restricción del acceso a la información
  - Procedimientos seguros de inicio de sesión
  - Sistema de gestión de contraseñas
  - Uso de utilidades con privilegios del sistema
  - Control de acceso al código fuente de los programas

6.8 CRIPTOGRAFÍA

La adecuada diligencia para garantizar un uso correcto y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información se manifiesta en el desarrollo y aplicación de los siguientes procesos documentados:

GSIGNE-SI-PR-10 Criptografía
THS-CL-AC-PR-20 TB01 Estructura de Certificados
THS-CL-AC-PR-21 TB02 Estructura CRL y Servicio OCSP
THS-CL-AC-CV-04 Ciclo vida certificados funcional
THS-CL-AC-DPC-01 PO02 Declaración de Prácticas de Certificación
THS-CL-AC-PR-05 Procedimiento de gestión de claves
THS-CL-AC-PR-02 PO03 Modelo operacional de la AC
THS-CL-AC-PR-03 PO04 Modelo operacional de la AR
THS-CL-AC-PR-10 Gestión de acceso a la CA
THS-CL-AC-PR-04 AD01 Manual de operaciones de la AC
THS-CL-AC-PR-06 AD02 Manual de operaciones de la AR
THS-CL-AC-PR-11 Backup y Restauración del HSM

En el documento interno GSIGNE-SI-PR-10 Criptografía, se describen los procesos de:

- Controles criptográficos
  - Política de uso de controles criptográficos de uso general
  - Gestión de Claves

6.9 SEGURIDAD FÍSICA Y DEL ENTORNO

Thomas-Signe para evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización, prevenir el acceso físico no autorizado, daños e interferencia a la información de la organización y a los recursos de tratamiento de la información, ha planificado los siguientes procesos descritos en los siguientes documentos:

GSIGNE-SI-PR-11 Seguridad fisica y del entorno
THS-CL-AC-PR-13 Seguridad física de la infraestructura PKI
GSIGNE-PR-GRAL-08 Políticas internas

En el documento interno GSIGNE-SI-PR-11 Seguridad Física y del entorno, se describen los procesos de:

- Áreas seguras del grupo
  - Perímetro de seguridad física
  - Controles físicos de entrada
  - Seguridad de oficinas, despachos y recursos
  - Protección contra las amenazas externas y ambientales
  - Trabajo en áreas seguras
  - Áreas de carga y descarga
- Seguridad en los equipos
  - Emplazamiento y protección de los equipos
  - Instalaciones de suministro
  - Seguridad del cableado
  - Mantenimiento de los equipos
  - Retirada de materiales propiedad de la empresa
  - Seguridad de los equipos fuera de las instalaciones
  - Reutilización o eliminación segura de los equipos
  - Equipo de usuario desatendido
  - Política de puesto de trabajo despejado y pantalla limpia

6.10 SEGURIDAD DE LAS OPERACIONES

Thomas Signe para asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, protegerlas contra el malware, manteniendo la integridad del software en explotación, Reduciendo los riesgos resultantes de la explotación de las vulnerabilidades técnicas y realizar una auditoria eficaz y eficiente sobre los sistemas ha desarrollado un conjunto de procesos descritos en los siguientes documentos:

GSIGNE-SI-PR-12 Seguridad de las Operaciones
GSIGNE-SI-PR-14 Adquisicion, desarrollo y mantenimiento
GSIGNE-TI-PR-02 Desarrollo
GSIGNE-PR-SI-41 Gestión de la Capacidad
Programación de hacking ético
GSIGNE-PR-GRAL-03 Auditoría

En este documento interno se describen los procesos de:

- Procedimientos y responsabilidades operacionales
  - Documentación de procedimientos de la operación
  - Gestión de cambios
  - Gestión de capacidades
  - Segregación de los recursos de desarrollo, prueba y operación
- Protección contra el software malicioso
- Copias de seguridad
- Registros y supervisión
  - Registro de eventos
  - Protección de la información de registros
  - Registro de administración y operación
  - Sincronización del reloj
- Control del software en explotación
- Gestión de la vulnerabilidad técnica
  - Gestión de vulnerabilidades técnicas
  - Restricción a la instalación de software
- Consideraciones sobre la auditoría de sistemas de información
- Protección del correo electrónico

6.11 SEGURIDAD DE LAS COMUNICACIONES

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de seguridad de las comunicaciones asociados al dominio 13 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-13 Seguridad de las Comunicaciones

En este documento interno se describen los procesos de:

- Gestión de la seguridad en las redes

  - Controles de red
  - Seguridad de los servicios de red
  - Segregación de redes
- Intercambio de información
  - Políticas y procedimientos de intercambio de información
  - Acuerdos de intercambio de información
  - Mensajería electrónica
  - Acuerdos de confidencialidad y no revelación
  - Borrado de metadatos

6.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de Adquisición, desarrollo y mantenimiento de los sistemas de información asociados al dominio 14 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-14 Adquisicion, desarrollo y mantenimiento

En este documento interno se describen los procesos de:

- Requisitos de seguridad en los sistemas de información
  - Análisis de requisitos y especificaciones de seguridad de la información
  - Asegurar los servicios de aplicaciones en redes públicas
  - Protección de las transacciones en los servicios de aplicaciones
- Seguridad en el desarrollo y en los procesos de soporte
  - Políticas de desarrollo seguro
  - Procedimiento de control de cambios en sistemas
  - Revisión técnica de las aplicaciones tras efectuar cambios en sistema operativo
  - Restricciones a los cambios en los paquetes software
  - Principios de ingeniería de desarrollo seguro
  - Entorno de desarrollo seguro
  - Externalización del desarrollo software
  - Pruebas funcionales de seguridad de sistemas
  - Pruebas de aceptación de sistemas
- Datos de prueba
  - Protección de los datos de prueba

6.13 RELACIÓN CON PROVEEDORES

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de Relación con Proveedores asociados al dominio 15 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-15 Relación con proveedores

En este documento interno se describen los procesos de:

- Seguridad en las relaciones con los proveedores
  - Política de seguridad de la información en las relaciones con los proveedores
  - Requisitos de seguridad en los contratos con terceros
  - Cadena de suministro de tecnología de la información y de las comunicaciones
- Identificación de los requisitos aplicables a terceros
  - Control y revisión de la provisión de servicios del proveedor
  - Gestión de los cambios en la provisión de servicios del proveedor

6.14 GESTIÓN DE INCIDENTES

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de Gestión de Incidentes asociados al dominio 16 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-16 Gestión de Incidentes.

En este documento interno se describen los procesos de:

- Gestión de incidentes de seguridad de la información
  - Responsabilidades y procedimientos
  - Notificación de eventos de seguridad de la información
  - Notificación de puntos débiles de seguridad de la información

  - Evaluación y decisión sobre los eventos de seguridad de la información
  - Respuesta a los incidentes de seguridad de la información
  - Aprendizaje de los incidentes de seguridad
  - Recopilación de evidencias
- Otros aspectos relacionados con la gestión de incidentes de seguridad de la información
  - Notificación a terceros de incidentes de seguridad
  - Toma de decisiones urgentes
  - Escalado de incidentes de seguridad

6.15 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de Gestión de Continuidad asociados al dominio 17 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-17 Aspectos de Seguridad de la Información para la GCN

En este documento interno se describen los procesos de:

- Continuidad de la seguridad de la información
  - Planificación de la continuidad de la seguridad de la información
  - Implementar la continuidad de la seguridad de la información
  - Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- Redundancias
  - Disponibilidad de los recursos de tratamiento de la información
- Contactos de interés
- Equipo de respuesta ante incidentes

6.16 CUMPLIMIENTO

La forma en que Thomas Signe como parte del grupo SIGNE cubre los controles asociados a los procesos de Cumplimiento asociados al dominio 18 del anexo de la norma ISO 27001, es desarrollado en los siguientes documentos:

GSIGNE-SI-PR-18 Cumplimiento

En este documento interno se describen los procesos de:

- Cumplimiento de los requisitos legales y reglamentarios
  - Identificación de la legislación aplicable y de los requisitos contractuales
  - Derechos de la propiedad intelectual
  - Protección de los registros de la organización
  - Protección y privacidad de la información de carácter personal
  - Regulación de controles criptográficos
- Revisiones de la seguridad de la información
  - Revisión independiente de la seguridad de la información
  - Cumplimiento de las políticas y normas de seguridad
  - Comprobación del cumplimiento técnico

6.17 COMITÉ DE SISTEMAS DE GESTIÓN

Con el objeto de asegurar el cumplimiento de esta Política de Seguridad de la Información, se establece una Estructura Organizacional de Seguridad de la Información que contempla la definición de funciones específicas en el ámbito de la seguridad.
Thomas Signe ha conformado el Comité de Sistemas de Gestión, el cual se debe encargar de aprobar las iniciativas de seguridad de la información y ciberseguridad y los riesgos que emanen de la gestión, adicionalmente deberá pronunciarse por las posibles desviaciones de la Política de Seguridad de la Información,

Las principales funciones del Comité son:

- Aprobar las Políticas de Seguridad.
- Aprobar el Sistema de Gestión de Seguridad de la Información.
- Informarse y pronunciarse sobre desviaciones derivada de la gestión de riesgos
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- Conocer y aprobar las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía.
- Notificar informar sobre cualquier situación irregular con respecto al servicio prestado por el PSC.

6.18 RELACIÓN ENTRE EL PLAN DE SEGURIDAD Y LOS RECURSOS ASIGNADOS

Thomas Signe tiene una adecuada relación entre recursos, sean estos humanos y materiales que le permiten gestionar de manera adecuada su plan de seguridad, en los planes de continuidad de negocio GSIGNE-SI-PR-17 Aspectos SI para la GCN y THS-CL-SI-PR-17 PS03 Plan de continuidad del Negocio, su sistema de gestión "GSIGNE-GRAL-MSG Manual de Sistemas de Gestion" y en la evaluación periódica de los planes y la gestión de riesgos que brinda el sistema de gestión de seguridad de la información basado en ISO 27001

7 TRAZABILIDAD ENTRE ISO 27002-POLÍTICA DE SEGURIDAD-DPC-PC

ISO/IEC 27002:2015 (Dominios)	Política de Seguridad	Política de Certificación	Declaración de Prácticas de Certificación
5. Políticas de seguridad de la información	Punto 6	Punto 6	9.6
6. Organización de la seguridad de la Información	Punto 6.4	Punto 6.3	Punto 9.6.1
7. Seguridad relativa a los recursos humanos	Punto 6.5	Punto 6.4	Punto 5.2 y 5.3
8. Gestión de activos	Punto 6.6	Punto 6.5	Punto 5
9. Control de acceso	Punto 6.7	Punto 6.6	Punto 6.5
10. Criptografía	Punto 6.8	Punto 6.7	Punto 6.5.1
11. Seguridad física y del entorno	Punto 6.9	Punto 6.8	Punto 5.1
12. Seguridad de las operaciones	Punto 6.10	Punto 6.9	Punto 5.4
13. Seguridad de las comunicaciones	Punto 6.11	Punto 6.10	Punto 6.7
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	Punto 6.12	Punto 6.11	Punto 6.6.1
15. Relación con proveedores	Punto 6.13	Punto 6.12	Punto 9.7.2
16. Gestión de incidentes	Punto 6.14	Punto 6.13	Punto 5.7
17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Punto 6.15	Punto 6.14	Punto 5.7
18. Cumplimiento	Punto 6.16	Punto 6.15	Punto 9.15 y 9.16

7.1 RELACIÓN DEL PLAN DE SEGURIDAD CON LAS PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

Las prácticas de certificación y las políticas de certificación son el resultado, de la coherencia de la gestión de seguridad de la información implementada mediante el sistema de gestión de seguridad de la información, del análisis y gestión de riesgos, de la continuidad de negocio y contienen lo indicado por la guía de acreditación y la RFC 3647.

8 FORMATOS

N/A

9 REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
N/A	N/A	N/A	N/A	N/A