Índice

Aprobación y entrada en vigor 2
Introducción 2
Alcances 2
Misión 3
Cumplimiento de artículos ENS 3
Marco normativo 3
Organización de la Seguridad 3
Comités: funciones y responsabilidades 3
El Departamento de Seguridad de GT 4
El Comité de Seguridad de CCA 6
Roles de seguridad 7
Director de Seguridad 7
Responsable de Seguridad (GT y ENS) 7
Responsable del Sistema ENS 8
Delegado de Protección de Datos 8
Procedimientos de designación 9
Política de Seguridad de la Información 9
Datos de carácter personal 10
Desarrollo de la Política de Seguridad de la Información 10
Terceras partes 10

Aprobación y entrada en vigor

Texto aprobado el día 27 de octubre de 2022 por el Comité de Seguridad. Esta Política de Seguridad de la Información es efectiva desde el 28 de octubre de 2022 y hasta que sea reemplazada por una nueva Política. Este texto anula el anterior, que fue aprobado el día 20 de enero de 2022 por el Comité de Dirección.

Introducción

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad, y autenticidad de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos dentro del alcance deben aplicar las medidas mínimas de seguridad exigidas tanto por la norma ISO 27001:2014 como por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los departamentos dentro del alcance deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de acuerdo al Artículo 7 del Esquema Nacional de Seguridad (ENS) y con el apartado 16.1 de la norma ISO 27002:2015.

Alcances

En lo que respecta al **Esquema Nacional de Seguridad**, el alcance es:

> *Los sistemas de información propiedad de "Trevenque, Sistemas de Información S.L.", que dan soporte a los servicios de:*
> - *Hosting y Housing*
> - *Provisión y mantenimiento de servidores privados virtuales (VPS)*
> - *Provisión y mantenimiento de servidores dedicados*
> - *Gestión de back-up*
>
> *de acuerdo la categorización del sistema vigente.*

Para este alcance, TREVENQUE ha decidido, para dar garantías de seguridad a los clientes del sector público, que **la categoría de los sistemas que soportan estos servicios es MEDIA**, conforme a lo establecido en el ANEXO I Categorías de los sistemas del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

En el caso de la **norma ISO 27001**, esta política se aplica a:

> Los sistemas de información que soportan los servicios de:
> - *Alojamiento físico de servidores de terceros.*
> - *Provisión y mantenimiento de servidores privados virtuales.*
> - *Provisión y mantenimiento de servidores dedicados.*
> - *Gestión de back up.*
> - *Co-ubicación de antenas de telecomunicación conforme a la declaración de aplicabilidad vigente.*

Misión

Desde su creación, TREVENQUE centra sus esfuerzos en poner a disposición de todos sus clientes un servicio informático integrado que facilite la gestión de sus sistemas como si de un departamento informático propio se tratase. Con esta apuesta, el cliente consigue un servicio personalizado de calidad con los servicios tecnológicos más innovadores y seguros.

Nuestro objetivo es lograr la satisfacción del cliente mediante la implantación de un sistema integral de gestión de la seguridad de la información y la calidad.

TREVENQUE mantiene sus compromisos de mejora continua en la seguridad de la información como elementos indispensables para lograr la confianza en sus productos y servicios, tomando como modelo de conducta los requisitos legalmente establecidos junto con la adecuación al Esquema Nacional de Seguridad, la implantación de las Normas ISO 27001, 9001 y 14001, así como otros códigos de buenas prácticas que pudiera suscribir.

Cumplimiento de artículos ENS

TREVENQUE para lograr el cumplimiento de los artículos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría MEDIA a alcanzar.

Estas medidas de seguridad se encuentran recogidas en el ANEXO II de esta Política de Seguridad de la Información.

Marco normativo

TREVENQUE se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código de Comercio, Código Civil, etc.) o específico.

Esta legislación aplicable se encuentra en el ANEXO I de esta Política de Seguridad de la Información.

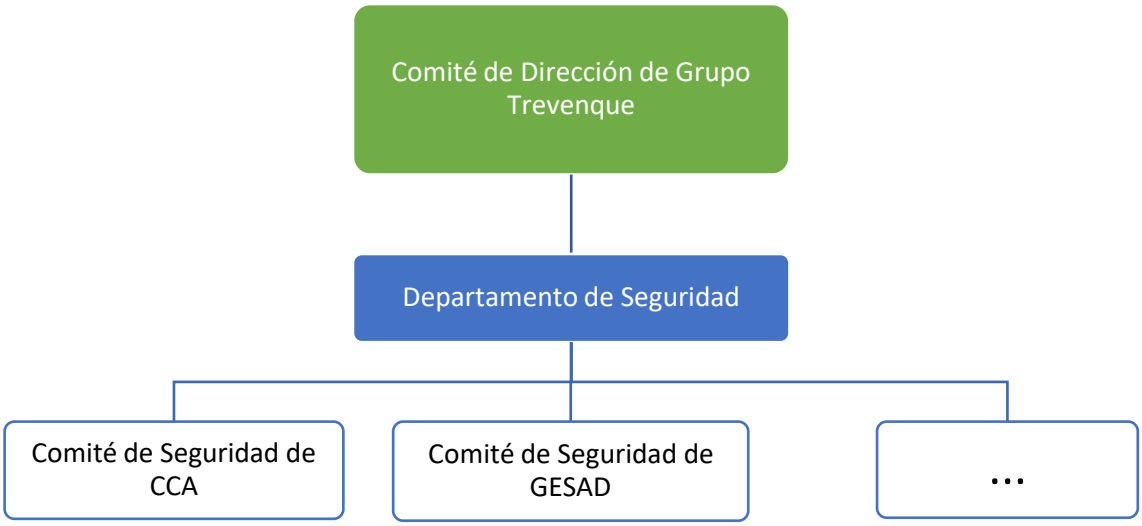
El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad de la Información, incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad”.

Serán los responsables de las distintas áreas técnicas del data-center los encargados de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

Organización de la Seguridad

Comités: funciones y responsabilidades

Se definen dos niveles de decisión para la correcta implantación de la seguridad en las distintas áreas del grupo cuya existencia dependerá de las necesidades regulatorias específicas de cada área.



En el primer nivel, un Comité de Seguridad específico por área. En este nivel se encuentra el **Comité de Seguridad de CCA**., con unos requisitos normativos y de servicio mucho mayores que el resto de las áreas del grupo. En caso de que otra área, bien transversal o de negocio, requiriese de un mayor control en este sentido, deberá comenzar por la creación de un Comité de Seguridad que se responsabilice de la definición, implantación y seguimiento de todos los asuntos relacionados con la Seguridad de la Información.

El Departamento de Seguridad de GT

En un segundo nivel se encuentra el **Departamento de Seguridad de GT**, que tiene como objetivo primordial coordinar la gestión de la seguridad de la información a nivel de organización. Este departamento se guiará por los objetivos estratégicos de la compañía y las buenas prácticas reconocidas en la industria de la ciberseguridad.

El Departamento de Seguridad de GT no es un comité técnico, pero recabará regularmente del personal técnico o jurídico, propio o externo, la información pertinente para tomar decisiones.

El Departamento de Seguridad de GT reportará al Comité de Dirección por medio de su Director de Seguridad, que forma parte del Comité de Dirección.

El Departamento de Seguridad de GT tendrá las siguientes funciones:

- Atender las inquietudes del Comité de Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información al Comité de Dirección.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por el Comité de Dirección.
- Aprobar la normativa de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Impulsar la cultura en seguridad de la información.

El Comité de Seguridad de CCA

El Comité de Seguridad de CCA estará formado por:

1. el Responsable de la Información y del Servicio (RIS).
2. el Responsable de Seguridad ENS (RSEG).
3. el Responsable de Sistema ENS (RSIS).

- podrán estar auxiliados de manera permanente o esporádica por consultores externos y/o el personal de la organización que se estime oportuno.

El presidente del Comité de Seguridad de CCA será el Responsable de la Información y del Servicio (RIS), para simplificar el proceso de firma de documentos podrá dar validez a los acuerdos del Comité firmando como "*Presidente, en representación del Comité de Seguridad de CCA*".

El secretario del Comité de Seguridad de CCA será el Responsable de Seguridad (RSEG) y tendrá como funciones: la convocatoria de las reuniones, la elaboración de las actas y la preparación de los temas a tratar aportando información puntual para la toma de decisiones. El Comité de Seguridad de CCA reportará al Comité de Dirección a través del presidente del Comité de Seguridad, presente en el Comité de Dirección.

El Comité de Seguridad de CCA tendrá una periodicidad **semestral** para las convocatorias ordinarias, sin que esto sea impedimento para que se realicen convocatorias extraordinarias de forma puntual a petición de cualquiera de los miembros del mismo.

El Comité de Seguridad de CCA tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de CCA y de sus diferentes áreas técnicas.
- Informar regularmente del estado de la seguridad de la información al Comité de Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas técnicas de CCA en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Monitorizar los principales riesgos residuales asumidos por la Dirección de CCA y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de CCA en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas técnicas de CCA, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Impulsar la cultura en seguridad de la información.

Roles de seguridad

A nivel de Grupo, transversal para toda la organización:

- Director de Seguridad.
- Responsable de Seguridad.
- Delegado de Protección de Datos.

A nivel de Comité de Seguridad de área, como en el Comité de Seguridad de CCA:

- **Responsable de la Información y del Servicio:** Representar en TREVENQUE las necesidades en materia de seguridad de la información, que le hayan sido trasladas por los Responsables de Información y Responsable de Servicios de los clientes sector público.
- **Responsable de Seguridad ENS**: encargado de la definición y validación de todos los aspectos de seguridad de los servicios dentro del alcance del ENS.
- **Responsable del Sistema ENS:** encargado operativa y adecuación de los servicios dentro del alcance a los requisitos del ENS.

Director de Seguridad

Las funciones del Director de Seguridad incluyen:

- Establecer los requisitos de la información en materia de seguridad, esto es, determinar los niveles de seguridad de la información.
- Establecer los requisitos del servicio en materia de seguridad, esto es, determinar los niveles de seguridad de los servicios que se proveen.
- Validar y aprobar los planes de mejora de la seguridad propuestos por el Responsable de Seguridad
- Validar y aprobar los planes de concienciación y formación propuestos por el Responsable de Seguridad.

El Director de Seguridad reporta directamente al Director General en materias de seguridad, no siendo esto óbice para que pueda reportar mensualmente al Comité de Dirección.

Responsable de Seguridad (GT y ENS)

El Responsable de Seguridad es el encargado de coordinar la aplicación de medidas de seguridad tomando las decisiones necesarias para satisfacer los requisitos de seguridad de la información y los servicios.
El Responsable de Seguridad reporta directamente al Director de Seguridad y al Comité de Seguridad.

Sus principales funciones son las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados.
- Realizar o promover las autoevaluaciones o auditorías periódicas que permitan verificar el cumplimiento del Esquema Nacional de Seguridad y la norma ISO 27001.
- Promover y gestionar la formación y concienciación en materia de seguridad TIC.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema, con el auxilio del resto del Comité de Seguridad.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para la alta dirección, incluyendo los incidentes más relevantes del periodo.

Responsable del Sistema ENS

El Responsable del Sistema es el encargado de la explotación tecnológica de la información tratada y los servicios prestados, el que opera y mantiene el sistema de información.

En materia de seguridad, el Responsable del Sistema, reporta al Responsable de Seguridad, sin embargo, no es su subordinado: aseguramos así la independencia, para que el Responsable del Sistema pueda tomar decisiones, como puede ser la parada de los servicios en el caso de que sea necesario.

- La aplicación y gestión de los Procedimientos Operativos de Seguridad, cuando así lo determine el Responsable de Seguridad,
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema.
- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema.
- Informar a los Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejo del sistema.
- Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo frecuentemente, de acuerdo con la política de seguridad establecida por la Organización.
- Asegurar el cumplimiento del proceso de respuesta ante incidentes de los actores bajo su responsabilidad, colaborando con el Responsable de Seguridad en la investigación de los mismos.
- Asumirá la **responsabilidad del Sistema de Gestión de Seguridad de la Información**, en caso de estar implantado.

Delegado de Protección de Datos

En el marco del Reglamento General de Protección de Datos se considera la figura del Delegado de Protección de Datos como el especialista en derecho de protección de datos.

El Delegado de Protección de Datos puede formar parte de la plantilla o ser un profesional ajeno que desempeñe sus funciones a través de un contrato de servicios. En todo caso, debe garantizarse su independencia: no puede recibir instrucciones, ni puede ser destituido ni sancionado por lo que respecta al desempeño de sus funciones. La independencia del DPD requiere que reporte directamente al más alto nivel de dirección sin necesidad de pasar por el filtro de mandos intermedios o superiores.

Debido a que el Delegado de Protección de Datos es una figura estratégica entre la empresa, el ciudadano y la Agencia de Protección de Datos, TREVENQUE ha decidido decantarse por un componente de la plantilla apoyado por proveedor externo que ayudará en tareas administrativas y de asesoría, en todo momento reportando al DPD interno.

Asimismo, considerando que el Delegado de Protección de Datos debe reportar directamente al Comité de Dirección y es altamente recomendable su participación en cualquier decisión relativa a la seguridad de los datos, TREVENQUE considera que el lugar indicado para ejercer este rol es el Comité de Seguridad.

El tercer criterio tenido en cuenta es la necesidad de eludir los cargos dentro de la organización en conflicto con el rol del Delegado de Protección de Datos, que serán aquellos cuyas responsabilidades incluyan determinar los fines y medios del tratamiento de datos personales.

Teniendo en cuenta todas estas consideraciones, TREVENQUE designa como Delegado de Protección de Datos al Responsable de Seguridad.

Procedimientos de designación

Los roles de Seguridad a nivel transversal serán nombrados por el Comité de Dirección, a propuesta del Comité de Seguridad, y pasarán a formar parte del Dpto. de Seguridad.

Los roles de seguridad específicos de cada área serán nombrados por el Comité de Dirección a propuesta del Comité de Seguridad, pero podrá delegar su nombramiento en los Directores de dichas áreas. La estructura de roles de seguridad a nivel de área estará compuesta por: un responsable de Información y Servicios, un responsable de Seguridad ENS y un responsable del Sistema ENS. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Política de Seguridad de la Información

Será misión del Comité de Seguridad de GT la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Comité de Dirección y difundida para que la conozcan todas las partes afectadas.

Datos de carácter personal

TREVENQUE sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido; de igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos. Estas medidas, recogidas en la documentación de seguridad que da cumplimiento a la normativa vigente, se integrarán en los procedimientos y su correspondiente gestión documental de la Seguridad de la Información de TREVENQUE.

Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información complementa las otras políticas de TREVENQUE entre las que figuran la de Calidad y Medio Ambiente y de cumplimiento de la normativa de protección de datos.

La Política de Seguridad se desarrollará por medio de normativa y procedimientos de seguridad que afronten aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Los Comités de Seguridad de área han aprobado el desarrollo de un sistema de gestión específico, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad y otros estándares de seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Terceras partes

Las terceras partes relacionadas con TREVENQUE, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando TREVENQUE utilice servicios de terceros o ceda información a terceros, además de trasladarles las obligaciones contractuales adquiridas con el cliente, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.