POLÍTICA

Política de Seguridad de la Información

Propietario	Responsable de Seguridad
Entrada en vigor	14/05/2026
Alcance	Todo el personal de la organización y terceras partes.

trevenque
group

Política de Seguridad de la Información. 2

Política de Seguridad de la Información.

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 14 de mayo de 2026 por el director de Trevenque Group. Esta Política de Seguridad de la Información es efectiva desde el 18 de mayo de 2026 y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior.

2. INTRODUCCIÓN

El objetivo de la **seguridad de la información** es garantizar la calidad de la información, la protección de los datos personales y la prestación continuada de los servicios, actuando de forma preventiva, supervisando la actividad diaria y reaccionando con agilidad ante los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para afectar a la confidencialidad, integridad, disponibilidad, trazabilidad, autenticidad de la información y los servicios, así como a los derechos y libertades de las personas cuyos datos personales son tratados. Para hacer frente a estas amenazas, se requiere una estrategia de seguridad dinámica que se adapte a los cambios del entorno, garantizando tanto la continuidad operativa como el cumplimiento normativo en materia de protección de datos.

Así, las distintas unidades organizativas de TREVENQUE GROUP deben aplicar las medidas de seguridad recomendadas por la norma ISO/IEC 27001:2022, el Esquema Nacional de Seguridad (ENS), y aquellas relativas a la gestión de datos personales conforme a la LOPDGDD. También deben llevar a cabo un seguimiento continuo de los niveles de prestación de servicios, gestionar adecuadamente las vulnerabilidades, y preparar respuestas eficaces ante incidentes que puedan comprometer tanto la seguridad como la privacidad de la información.

Los departamentos dentro del alcance deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, en línea con lo establecido en el Artículo 8 del Esquema Nacional de Seguridad, asegurando además el respeto de los principios de minimización, limitación, licitud y responsabilidad proactiva en el tratamiento de datos personales.

3. MISIÓN

Desde su creación, TREVENQUE GROUP 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.

TREVENQUE GROUP mantiene sus compromisos de mejora continua en 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, 27017 y 27018, así como otros códigos de buenas prácticas que pudiera suscribir.

4. DATOS DE CARÁCTER PERSONAL Y COMPROMISO CON LA PRIVACIDAD

4.1. Compromiso de la Dirección

La Dirección de TREVENQUE GROUP manifiesta su firme liderazgo y compromiso con la protección de los datos personales tratados por la organización, tanto de empleados como de clientes, proveedores y otras partes interesadas. Este compromiso se traduce en la integración de la gestión de la privacidad en todos los niveles organizativos, asegurando la disponibilidad de recursos necesarios y promoviendo una cultura de respeto y responsabilidad hacia la información personal.

Los Principios Rectores de TREVENQUE GROUP en materia de protección de datos son:

1. Legalidad, lealtad y transparencia en el tratamiento de los datos personales.
2. Limitación de la finalidad y minimización de datos, asegurando que se recojan únicamente los datos pertinentes y necesarios.
3. Exactitud, integridad y confidencialidad, así como el compromiso con la limitación del plazo de conservación.
4. Responsabilidad proactiva y enfoque basado en riesgos, adoptando las medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado de protección.

Así, TREVENQUE GROUP 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 GROUP.

4.2. Protección de datos personales en la nube pública (ISO 27018)

TREVENQUE GROUP, asimismo, trasladará el cumplimiento de la legislación aplicable en materia de protección de datos personales a las condiciones contractuales acordadas con los clientes cuando TREVENQUE GROUP actúe como encargado del tratamiento en la nube pública.

Los acuerdos contractuales asignarán claramente responsabilidades entre TREVENQUE GROUP, sus subcontratistas y el cliente, considerando el modelo de servicio (IaaS, PaaS o SaaS). En particular, la asignación de responsabilidades sobre los controles de la capa de aplicación se definirá en función del modelo de servicio prestado.

5. CUMPLIMIENTO DE ARTÍCULOS ENS

TREVENQUE para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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 **ALTA** a alcanzar.

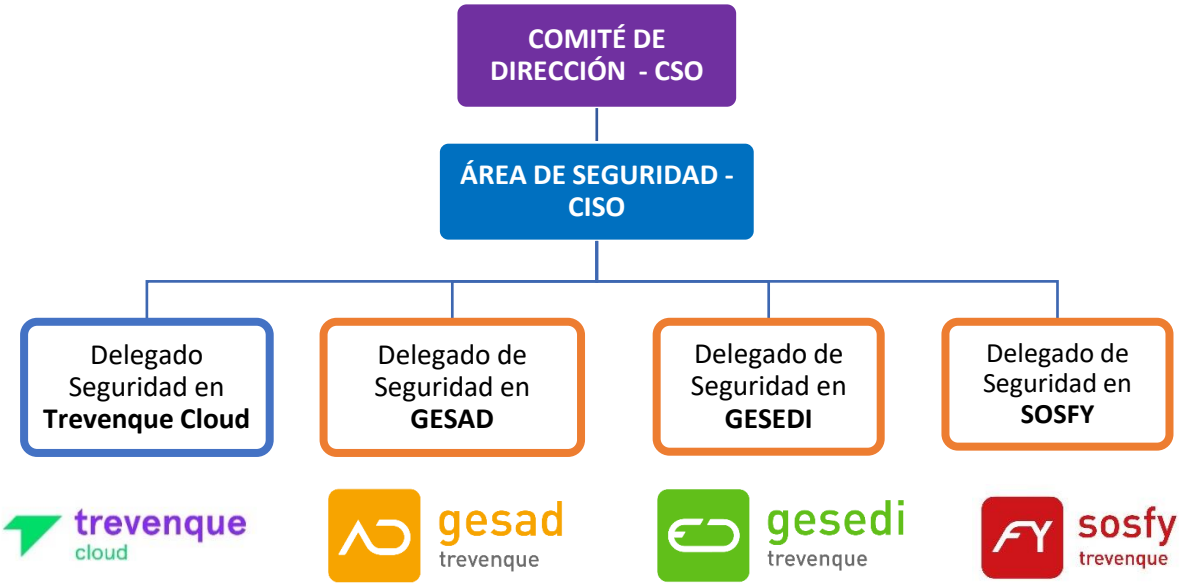
5.1. Marco normativo

TREVENQUE GROUP 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 CISO, incluido las instrucciones técnicas de seguridad (ITS) 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. Serán los responsables de las distintas áreas técnicas los encargados de identificar las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. 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 se encuentran los delegados de seguridad específicos de cada área, involucrados en el día a día de las mismas, reportando al CISO de la compañía en el ejercicio de este rol; desde ahí se hacen efectivas las políticas de seguridad hacia el resto del grupo. Todos los departamentos o unidades organizativas de la compañía que requieran de un mayor control en este sentido deberá comenzar por adopción de un modelo similar con un delegado de seguridad dependiente del área de Seguridad y GRC de Trevenque Group, que se responsabilizará de la implantación y seguimiento de todos los asuntos relacionados con la Seguridad de la Información.

6.1.1. El área de Seguridad y GRC de Trevenque Group

En un segundo nivel se encuentra el **ÁREA DE SEGURIDAD Y GRC**, 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 área de Seguridad y GRC no es un comité exclusivamente técnico, pero recabará regularmente del personal técnico o jurídico, propio o externo, la información pertinente para tomar decisiones. Reportará al Comité de Dirección por medio de su director de Seguridad (CSO), que forma parte del Comité de Dirección.

El área de Seguridad y GRC 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.

6.1.2. Arquitectura de seguridad de las áreas

El diseño de la función de Seguridad en las áreas de Trevenque Group estará formado por:

1. el responsable de la Información y del Servicio.
2. el delegado de Seguridad.
3. el responsable de Sistema.

podrán estar auxiliados de manera permanente o esporádica por consultores externos y/o el personal de la organización que se estime oportuno, en especial del área de Seguridad y GRC o, en su caso, el DPD.

El delegado de seguridad actuará en representación del Responsable de Seguridad (CISO) y los intereses del área de Seguridad y GRC, reportando directamente al CISO en el ejercicio de este rol. El delegado se integrará de la forma que considere más oportuna en los procesos y actividades del área para alcanzar sus objetivos de seguridad.

Esta arquitectura, compuesta por los tres roles de seguridad mencionados tendrá las siguientes funciones:

- Atender las inquietudes del área de Seguridad y GRC en el lo referente a Seguridad de la información, así como al cumplimiento normativo.
- Informar regularmente del estado de la seguridad de la información al CISO.
- Promover la mejora continua del sistema de gestión de la seguridad y provacidad de la información.
- Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones al respecto.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto.
- 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 del área, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Impulsar la cultura en seguridad de la información.

6.2. Roles de seguridad

Los roles, a nivel de Grupo, transversales para toda la organización:

- Director de Seguridad (CSO).
- Responsable de Seguridad (CISO).
- Delegado de Protección de Datos (DPD).

Los roles a nivel de área:

- **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 del sector público.
- **Delegado de Seguridad**: encargado de la implantación y validación de todos los aspectos de seguridad de los servicios con necesidades especiales de regulación.
- **Responsable del Sistema:** encargado de la operativa y adecuación de los servicios dentro del alcance a los requisitos normativos.

6.2.1. Director de Seguridad (CSO)

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. Sus funciones 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.

6.2.2. Responsable de Seguridad (CISO)

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. 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 las normas ISO 27001 y 27701.
- 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 área de Seguridad y GRC y los delegados 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.

6.2.3. Responsable del Sistema

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 delegado 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 al 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.

6.2.4. Delegado de Protección de Datos

4. el responsable de la Información y del Servicio.
5. el delegado de Seguridad.
6. el responsable de Sistema.

podrán estar auxiliados de manera permanente o esporádica por consultores externos y/o el personal de la organización que se estime oportuno, en especial del área de Seguridad y GRC o, en su caso, el DPD.

El delegado de seguridad actuará en representación del Responsable de Seguridad (CISO) y los intereses del área de Seguridad y GRC, reportando directamente al CISO en el ejercicio de este rol. El delegado se integrará de la forma que considere más oportuna en los procesos y actividades del área para alcanzar sus objetivos de seguridad.

Esta arquitectura, compuesta por los tres roles de seguridad mencionados tendrá las siguientes funciones:

- Atender las inquietudes del área de Seguridad y GRC en el lo referente a Seguridad de la información, así como al cumplimiento normativo.
- Informar regularmente del estado de la seguridad de la información al CISO.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones al respecto.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto.
- 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 del área, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Impulsar la cultura en seguridad de la información.

6.3. Roles de seguridad

Los roles, a nivel de Grupo, transversales para toda la organización:

- Director de Seguridad (CSO).
- Responsable de Seguridad (CISO).
- Delegado de Protección de Datos (DPD).

Los roles a nivel de área:

- **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 del sector público.
- **Delegado de Seguridad**: encargado de la implantación y validación de todos los aspectos de seguridad de los servicios con necesidades especiales de regulación.
- **Responsable del Sistema:** encargado de la operativa y adecuación de los servicios dentro del alcance a los requisitos normativos.

6.3.1. Director de Seguridad (CSO)

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. Sus funciones 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.

6.3.2. Responsable de Seguridad (CISO)

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. 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 las normas ISO 27001, 27017 y 27018.
- 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 área de Seguridad y GRC y los delegados 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.

6.3.3. Responsable del Sistema

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 delegado 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 al 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.

6.3.4. 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.

Un factor crítico a tener 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.

Debido a la importancia que la compañía le otorga al correcto tratamiento de la información personal, junto al hecho de que el delegado de Protección de Datos es una figura estratégica entre la empresa, el ciudadano y la Agencia de Protección de Datos, TREVENQUE GROUP ha decidido contratar un proveedor especializado que ejercerá de DPD, apoyado y coordinado por un enlace interno desde el área Legal.

Procedimientos de designación

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

Los roles de seguridad específicos de cada área serán nombrados por el Comité de Dirección a propuesta del CISO, que se basará en la opinión de 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 delegado de seguridad y un responsable del Sistema. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Política de Seguridad de la Información

Será misión del CISO de TREVENQUE GROUP 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.

7. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las otras políticas de TREVENQUE GROUP 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.

El área de Seguridad y GRC ha diseñado un sistema de gestión integral para toda la compañía, 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.

8. TERCERAS PARTES

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

Cuando TREVENQUE GROUP 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.

En el caso de que dichas terceras partes participen en la prestación de servicios en la nube y/o en el tratamiento de datos personales, los acuerdos deberán reflejar de forma explícita la asignación de responsabilidades y los requisitos de seguridad aplicables, incluyendo, cuando proceda, obligaciones de notificación de incidentes y soporte a investigaciones.

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.

9. SERVICIOS EN LA NUBE

Cuando TREVENQUE GROUP diseñe, implante, opere o preste servicios en la nube, definirá los procedimientos específicos que aborden la prestación y el uso de dichos servicios, en línea con ISO/IEC 27017.

- Los requisitos básicos de seguridad de la información aplicables al diseño y aplicación del servicio en la nube.
- La gestión del riesgo asociado al personal con privilegios (personas con información privilegiada autorizada).
- El aislamiento entre clientes y los entornos multi-tenant, incluyendo la virtualización.
- Las condiciones de acceso del personal de TREVENQUE GROUP a los activos y datos del cliente, limitándolo a lo estrictamente necesario y garantizando su trazabilidad.
- Los procedimientos de control de acceso, incluyendo autenticación reforzada para el acceso administrativo a los servicios en la nube.
- Las comunicaciones a los clientes durante la gestión del cambio que pueda afectar a la seguridad, continuidad o privacidad del servicio.
- La seguridad de la virtualización (ciclo de vida de instancias, imágenes y *snapshots*, protección de hipervisores y control de portales de autoservicio).
- El acceso y la protección de los datos de los clientes de servicios en la nube.
- La gestión del ciclo de vida de las cuentas de clientes de servicios en la nube.

La comunicación de infracciones y las pautas de intercambio de información para apoyar investigaciones y análisis forenses, de acuerdo con la legislación y los contratos aplicables.