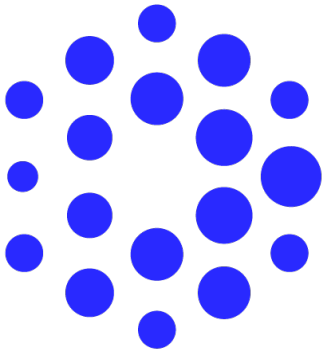

FRACTTAL

Política de Seguridad de la Información (ENS)

Área de Seguridad y Nuevas Tecnologías

Política de Seguridad de la Información ENS				
Versión:	**1.1**	Fecha:	**22/05/2026**	FRACTTAL
Clasificación del documento: **USO INTERNO**				

CONTENIDO

Política de Seguridad de la Información ENS				
Versión:	**1.1**	Fecha:	**22/05/2026**	FRACTTAL
Clasificación del documento: **USO INTERNO**				

1. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Referencias	Realizado	Aprobado
1.0	23/04/2026	Elaboración del documento	org. 1	Responsable de Seguridad	Dirección
1.1	22/05/2026	Modificacion del documento - responsable de seguridad	org. 1	Responsable de Seguridad	Dirección

2. EXPOSICIÓN DE MOTIVOS

FRACTTAL, como empresa de servicios de gestión de mantenimiento, desarrolla su actividad con el objetivo de garantizar la continuidad, calidad y seguridad de los servicios que presta.

Las plataformas, sistemas y redes que soportan estos servicios deben diseñarse, implementarse y operarse con la máxima diligencia, adoptando medidas adecuadas desde las fases iniciales de concepción y diseño para protegerlos frente a daños accidentales o ataques deliberados que puedan afectar a la **disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad** de la información, los productos desarrollados o los servicios prestados.

El objetivo de la Seguridad de la Información en FRACTTAL es asegurar la resiliencia organizativa, preservar la reputación corporativa, garantizar la calidad de la información y del software o sistemas desplegados, así como mantener la prestación continuada de los servicios críticos. Esto se consigue actuando preventivamente, supervisando de forma constante la actividad diaria y reaccionando con rapidez y eficacia ante cualquier incidente.

Para hacer frente a las amenazas, FRACTTAL adopta una estrategia dinámica capaz de adaptarse a los cambios tecnológicos, regulatorios y operativos del entorno. Esto implica que todos los departamentos deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), realizar un seguimiento continuo de la calidad de las infraestructuras y servicios, analizar y corregir las vulnerabilidades detectadas, y preparar respuestas efectivas ante incidentes de seguridad.

Los distintos equipos de la organización velarán por que la seguridad TIC sea un componente integral en todas las fases del ciclo de vida de los sistemas: desde la concepción, el desarrollo o adquisición, hasta la operación y eventual retirada de servicio. Los requisitos de seguridad y los recursos necesarios para su financiación deberán identificarse e incluirse en la planificación, en las solicitudes de oferta y en los pliegos de licitación de proyectos TIC.

Asimismo, deberán estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, conforme a lo establecido en los Artículos 7 y 8 del ENS.

Para todo ello, FRACTTAL cuenta con un Sistema de Gestión de la Seguridad de la Información basado en el Esquema Nacional de Seguridad, que sigue un ciclo de mejora continua.

3. MISIÓN

Ofrecer a las empresas y administraciones públicas un servicio de gestión de mantenimiento con los mayores estándares de calidad y garantías de continuidad, con un firme compromiso con la protección de la información.

4. ALCANCE Y CATEGORÍA DEL SISTEMA

La presente Política de Seguridad aplica a la gestión de la seguridad de la información y los controles técnicos en nuestras soluciones de SaaS, Fracttal One para la gestión de mantenimientos de activos implementados en nubes públicas, para la protección de los activos de información de clientes, y de los segmentos de Energía, Hoteles, Transporte, Salud y Servicios. La seguridad de la información de Fracttal se extiende además a las siguientes áreas funcionales: Operaciones, Recursos Humanos, Legal y Tecnología, y a los siguientes procesos: Proceso de Desarrollo, Procesos de Operaciones de TI y Proceso de Operaciones. La seguridad aplicada va desde la recepción de información, creación, procesamiento, transferencia, hasta su resguardo.

De acuerdo con el procedimiento de categorización establecido en el Anexo I del Real Decreto 311/2022, los sistemas de información incluidos en el alcance han sido categorizados como de categoría MEDIA, al alcanzar al menos una de sus dimensiones de seguridad el nivel MEDIO, conforme al procedimiento establecido en el Anexo I del Real Decreto 311/2022.

5. PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS

FRACTTAL asume y hace propios los principios básicos y requisitos mínimos establecidos en los Capítulos II y III del Real Decreto 311/2022, que inspiran y rigen la presente Política:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en lo relativo al funcionamiento electrónico del sector público, registros y notificaciones).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

5.1. PRINCIPIOS BÁSICOS (arts. 5 a 10 del ENS)

- **Seguridad como proceso integral**: la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, técnicos, materiales y organizativos relacionados con el sistema (art. 5).
- **Gestión de la seguridad basada en los riesgos**: el análisis y gestión de riesgos es parte esencial del proceso de seguridad y debe mantenerse permanentemente actualizado (art. 6).

- **Prevención, detección, respuesta y conservación**: la seguridad del sistema debe contemplar las acciones de prevención, detección y respuesta ante incidentes, así como la conservación de la información (arts. 7 y 8).
- **Existencia de líneas de defensa**: el sistema debe disponer de una estrategia de protección constituida por múltiples capas de seguridad (art. 9).
- **Vigilancia continua y reevaluación periódica**: la vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta, y la evaluación permanente del estado de la seguridad (art. 10).

5.2. REQUISITOS MÍNIMOS (arts. 11 a 27 del ENS)

La presente Política contempla los requisitos mínimos de seguridad establecidos en el Capítulo III del ENS, que se desarrollan en la normativa y procedimientos del Sistema de Gestión de la Seguridad de la Información, incluyendo entre otros: organización e implantación del proceso de seguridad, análisis y gestión de riesgos, gestión de personal, profesionalidad, autorización y control de los accesos, protección de las instalaciones, adquisición de productos y contratación de servicios de seguridad, mínimo privilegio, integridad y actualización del sistema, protección de la información almacenada y en tránsito, prevención ante otros sistemas de información interconectados, registro de la actividad y gestión de incidentes de seguridad, continuidad de la actividad, y mejora continua del proceso de seguridad.

6. MARCO NORMATIVO

Como base normativa para la elaboración de la presente Política de Seguridad de la Información, Fracttal ha analizado la legislación vigente que resulta de aplicación a su actividad como proveedor de servicios digitales y plataforma SaaS, en particular aquella relacionada con la seguridad de la información, la protección de datos personales, la administración electrónica, la identificación y los servicios electrónicos de confianza.

Este marco normativo sirve de referencia para la implantación de medidas de seguridad técnicas y organizativas en los sistemas de información que soportan los servicios prestados por Fracttal, de conformidad con el Esquema Nacional de Seguridad (ENS).

Como base normativa para realizar la presente Política de Seguridad, se ha analizado la legislación vigente que afecta al desarrollo de las actividades de la organización en lo que a administración electrónica y seguridad de la información se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal viene establecido por la siguiente legislación:

I. Procedimiento administrativo

(aplicable como marco de referencia para la relación con las Administraciones Públicas)

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

II. Protección de datos de carácter personal

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

III. Seguridad de los sistemas de información

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2). *A fecha de esta Política aún no ha sido traspuesta al ordenamiento jurídico español, por lo que todavía no es de aplicación.*

IV. Identificación electrónica, firma y servicios electrónicos de confianza

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS).
- Reglamento (UE) 2024/1183, del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 y se establece el marco europeo de identidad digital.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

V. Normativa relativa a la inteligencia artificial

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial

VI. Marcos de referencia y buenas prácticas internacionales

Con carácter complementario, Fracttal toma como referencia las siguientes guías y recomendaciones internacionales, en la medida en que resultan coherentes con el ENS y con el Sistema de Gestión de la Seguridad de la Información:

- Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad.

- Como complemento a la legislación vigente, se toman como referencia las normas internacionales UNE-ISO/IEC 27001 y UNE-ISO/IEC 27002, así como las guías CCN-STIC del Centro Criptológico Nacional.

Estas guías no tienen carácter normativo obligatorio, pero se consideran buenas prácticas reconocidas internacionalmente para reforzar la gestión de la seguridad de la información.

7. DEFINICIONES Y ACRÓNIMOS

Acrónimo	Definición
ENS	Esquema Nacional de Seguridad (Real Decreto 311/2022)
SGSI	Sistema de Gestión de la Seguridad de la Información
CCN	Centro Criptológico Nacional
CCN-CERT	Equipo de Respuesta ante Incidentes de Seguridad del CCN
INCIBECERT	Equipo de Respuesta ante Incidentes de Seguridad de INCIBE, CSIRT de referencia para el sector privado
RGPD	Reglamento General de Protección de Datos (Reglamento UE 2016/679)
LOPDGDD	Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
eIDAS	Reglamento (UE) 910/2014 de identificación electrónica y servicios de confianza
NIS2	Directiva (UE) 2022/2555 de ciberseguridad
RAT	Registro de Actividades del Tratamiento

8. DOCUMENTACIÓN Y DESARROLLO NORMATIVO

El cuerpo normativo de seguridad de la información de FRACTTAL se estructura en los siguientes niveles jerárquicos:

- **Nivel 1 - Política de Seguridad de la Información:** documento de máximo nivel que establece los principios, directrices y compromisos en materia de seguridad. Es aprobada por la Dirección.
- **Nivel 2 – Políticas o Normativas de Seguridad:** desarrollan la Política en ámbitos concretos (control de accesos, clasificación de la información, uso aceptable, etc.). Son aprobadas por el Comité de Seguridad.
- **Nivel 3 - Procedimientos operativos de seguridad:** describen las tareas concretas y los pasos a seguir para la implementación de las normativas. Son elaborados por el Responsable de Seguridad, el responsable del Sistema o los Administradores de Seguridad del Sistema, según su ámbito de competencia, y aprobados por el responsable de Seguridad.
- **Nivel 4 - Registros e informes:** evidencias del funcionamiento del SGSI (registros de incidentes, actas, informes de auditoría, resultados de análisis de riesgos, etc.).

El conjunto de esta documentación constituye el repositorio documental del SGSI y estará disponible para todo el personal que lo necesite en el ejercicio de sus funciones.

9. ORGANIZACIÓN DE SEGURIDAD

9.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad es el órgano que coordina la Seguridad de la Información a nivel de la organización. Estará constituido por el responsable de Seguridad de la Información y por representantes de otras áreas afectadas por el ENS.

Funciones del Comité

- Elaborar, revisar y proponer la Política de Seguridad para su aprobación por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad.
- Monitorizar los principales riesgos residuales asumidos por la organización.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad.
- Promover la realización de las auditorías periódicas de cumplimiento.
- Aprobar planes de mejora de la seguridad con sus dotaciones presupuestarias.
- Velar porque la seguridad se tenga en cuenta en todos los proyectos TIC desde su especificación inicial.
- Resolver los conflictos de responsabilidad entre los diferentes responsables o áreas.
- Informar regularmente del estado de la seguridad a la Dirección.
- Promover la mejora continua del SGSI.

Composición del Comité

Posición / Rol	Nombre	Fecha[1]
Presidencia	Christian Struve	31/03/2026
Responsable de Seguridad	Carlos Jaramillo Pereira	22/05/2026
Responsable del Sistema	Edwin Montoya Jaramillo	31/03/2026
Responsable de la Información	Santiago Herrera	31/03/2026
Responsable del Servicio	Alejandro Pérez	31/03/2026
Responsable de Protección de Datos	Grupo Ático 34	31/03/2026
Administrador de Seguridad del Sistema	Ana María Pérez	31/03/2026

9.2. DEFINICIÓN DE ROLES Y RESPONSABILIDADES

Se establecen los siguientes roles en la organización, conforme al Anexo II del ENS (medida [org.1]). Las funciones detalladas, requisitos de compatibilidad y mecanismos de delegación de cada rol se desarrollan en el documento *"Normativa Roles y Responsabilidades de Seguridad de la Información ENS*".

Las funciones detalladas de cada rol se han externalizado a dicho documento normativo específico, reduciendo la extensión de la Política y facilitando su mantenimiento. **Presidencia del Comité**

El CEO de FRACTTAL preside el Comité de Seguridad de la Información. Su Presidente es la máxima autoridad en materia de seguridad de la información dentro de la organización, y tiene voto de calidad en caso de desacuerdos. **Responsable de la Información**

Tiene la responsabilidad última del uso que se haga de una cierta información y, por lo tanto, de su protección. Establece los requisitos de la información en materia de seguridad, lo que en el marco del ENS equivale a determinar los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del ENS. Este rol podrá coincidir con el de Responsable del Servicio y con el de responsable del tratamiento requerido por el RGPD. No coincidirá con el de Responsable de Seguridad, excepto en organizaciones de reducida dimensión. **Responsable del Servicio**

Tiene la responsabilidad última del uso que se haga de determinados servicios y, por lo tanto, de su protección. Establece los requisitos de los servicios en materia de seguridad y determina los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del ENS.

Responsable de Seguridad de la Información

Actúa como Secretario del Comité de Seguridad. Es responsable de mantener la seguridad de la información y de los servicios prestados, promover la formación y concienciación, realizar el análisis de riesgos, elaborar la Declaración de Aplicabilidad (SoA), coordinar la documentación de seguridad y facilitar periódicamente al Comité un resumen de actuaciones e incidentes. **Responsable del Sistema**

[1] *Fecha de Adhesión al Comité de Seguridad de la Información*

Responsable de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Define la topología y sistema de gestión, y se asegura de que las medidas de seguridad se integren adecuadamente. Puede acordar la suspensión del uso de información o prestación de un servicio si es informado de deficiencias graves de seguridad. **Responsable en materia de protección de datos**

FRACTTAL ha optado por disponer de un Responsable de Protección de Datos, cuyas funciones se alinean con las establecidas en el artículo 39 del RGPD: informar y asesorar, supervisar el cumplimiento normativo, ofrecer asesoramiento sobre evaluaciones de impacto, cooperar con la autoridad de control y actuar como punto de contacto de la misma.

Administrador de la Seguridad del Sistema

Responsable de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información. Asegura que los controles de seguridad sean cumplidos, que la trazabilidad y pistas de auditoría estén habilitadas, y monitoriza el estado de la seguridad del sistema.

10. DATOS DE CARÁCTER PERSONAL

FRACTTAL trata datos de carácter personal. Disponemos de un Registro de Actividades del Tratamiento (RAT) que ha sido realizado con un modelo RoPA que incluye el análisis de criticidad de los datos tratados por nuestra organización, donde se recogen los tratamientos afectados y los correspondientes responsables. Todos los sistemas de información de FRACTTAL se ajustarán a los niveles de seguridad requeridos por la normativa en función de la naturaleza y finalidad de los datos de carácter personal tratados.

11. GESTIÓN DE RIESGOS

Justificación

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los cuales están expuestos. El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 7 del ENS. **Criterios de evaluación de riesgos**

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejada y los diferentes servicios prestados. Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos elaborada por la organización, basándose en estándares y buenas prácticas reconocidas (MAGERIT, ISO 27005). **Proceso de aceptación del riesgo residual**

Los niveles de riesgo residual resultantes del análisis de riesgos, que contempla todos los activos que integran los sistemas de información (información, servicios, hardware, software, comunicaciones, personas, instalaciones, medios auxiliares, proveedores, etc.), después de la

implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad del Anexo II del ENS), deberán ser aceptados formalmente por sus respectivos dueños. Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad al Comité de Seguridad para su evaluación, aprobación o rectificación. **Necesidad de realizar o actualizar evaluaciones de riesgos**

El análisis de riesgos se repetirá al menos una vez al año, y siempre que se produzcan cambios significativos en la información manejada, los servicios prestados, los sistemas que los soportan, cuando ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD

Prevención

Los departamentos deben evitar, o al menos prevenir en lo posible, que la información, los productos desarrollados o los servicios prestados se vean perjudicados por incidentes de seguridad. El ENS, a través de su artículo 19, establece que los sistemas deben diseñarse y configurarse garantizando la seguridad por defecto, en línea con la política de mínimo privilegio. Los departamentos deben implementar las medidas mínimas determinadas por el ENS, así como cualquier control adicional identificado a través del análisis de riesgos. **Detección**

Deben establecerse mecanismos de monitorización continua para detectar anomalías en los niveles de prestación de los servicios, así como cambios o accesos no autorizados a los repositorios de código y activos de información, actuando en consecuencia según lo establecido en el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte, incluyendo sistemas de detección de intrusos a nivel de red y de sistema. **Respuesta**

FRACTTAL, a través de sus diferentes departamentos, establece mecanismos para responder eficazmente a los incidentes de seguridad, designa un punto único de contacto para las comunicaciones relativas a incidentes y establece protocolos para el intercambio de información, incluyendo comunicaciones con los Equipos de Respuesta a Emergencias (CERT). **Notificación de incidentes de seguridad**

De conformidad con el artículo 33.7 del RD 311/2022, FRACTTAL, como entidad del sector privado que presta servicios a entidades públicas, notificará al INCIBE-CERT - centro de respuesta a incidentes de seguridad de referencia para ciudadanos y entidades de derecho privado, operado por el Instituto Nacional de Ciberseguridad de España - aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.

INCIBE-CERT pondrá inmediatamente en conocimiento del CCN-CERT los incidentes notificados, conforme al mecanismo de coordinación establecido en la normativa vigente (RD 43/2021 y Guía Nacional de Notificación y Gestión de Ciber incidentes). Se notificarán de forma obligatoria los incidentes con nivel de impacto Crítico, Muy Alto o Alto, conforme a los criterios de la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad. **Recuperación**

Para asegurar el correcto restablecimiento de los servicios, FRACTTAL desarrollará y mantendrá un análisis de impacto (*BIA*) que identifique los servicios esenciales, los activos críticos que los soportan, los requisitos mínimos de recuperación, el tiempo máximo tolerable de interrupción (*RTO*) y la pérdida de datos admisible (*RPO*).

13. OBLIGACIONES DEL PERSONAL

Todos los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad que la desarrolla. Es responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de la organización, constituyendo su incumplimiento una infracción grave a efectos laborales, conforme al convenio colectivo laboral aplicable.

14. CUMPLIMIENTO Y RÉGIMEN DISCIPLINARIO

El incumplimiento de la presente Política de Seguridad y de la normativa que la desarrolla podrá dar lugar a la aplicación de las medidas disciplinarias previstas en la legislación laboral vigente y en el convenio colectivo de aplicación, sin perjuicio de las responsabilidades civiles, penales o administrativas que pudieran derivarse.

El responsable de Seguridad, en coordinación con el Comité de Seguridad de la Información y los departamentos de Recursos Humanos y Jurídico, velará por que se inicien los procedimientos disciplinarios oportunos cuando se detecten incumplimientos de la normativa de seguridad.

15. FORMACIÓN Y CONCIENCIACIÓN

El objetivo de FRACTTAL es concienciar de forma continua en la ciberseguridad a los empleados, para ello se realiza:

- Formación inicial a la incorporación de los empleados a la organización.
- Envío periódico de píldoras de concienciación en ciberseguridad.
- Envío periódico de píldoras informativas de ciberseguridad, respondiendo a situaciones de riesgo.
- Formación anual a todo el personal de actualización en seguridad de la información.
- Formación específica según el puesto de trabajo y necesidades concretas.

La Dirección se compromete a dotar los recursos necesarios para la formación y concienciación del personal de FRACTTAL.

16. TERCERAS PARTES Y CADENA DE SUMINISTRO

FRACTTAL adquiere un especial compromiso en la gestión de la seguridad con terceras partes:

- Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipes de esta Política, se establecerán canales de reporte y coordinación y se establecerán procedimientos de actuación para la reacción ante incidentes.
- Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta Política y de la normativa de seguridad que concierna a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas.
- Se establecerán procedimientos específicos de reporte y resolución de incidencias.
- Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que establece esta Política.
- Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos y la forma de tratarlos, que deberá ser aprobado por los responsables de la información y los servicios afectados.

De conformidad con el artículo 2.3 del RD 311/2022, cuando FRACTTAL preste servicios o provea soluciones a otras entidades del sector público, los sistemas de información utilizados deberán cumplir con el ENS. Asimismo, FRACTTAL velará por que sus proveedores y subcontratistas que accedan a información o sistemas incluidos en el alcance del ENS mantengan niveles de seguridad equivalentes a los exigidos por esta Política.

17. AUDITORÍA DE CONFORMIDAD CON EL ENS

De conformidad con el artículo 31 del Real Decreto 311/2022, los sistemas de información de categoría MEDIA serán objeto de una **auditoría regular ordinaria al menos cada dos años** que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse una auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años de la siguiente auditoría regular ordinaria.

Los informes de auditoría serán presentados al responsable de Seguridad y al Comité de Seguridad de la Información, quienes adoptarán las medidas correctoras oportunas.

18. CONFORMIDAD Y CERTIFICACIÓN ENS

FRACTTAL tiene como objetivo obtener y mantener la certificación de conformidad con el Esquema Nacional de Seguridad para los sistemas de información incluidos en el alcance de la presente Política, conforme a lo establecido en el artículo 38 del RD 311/2022 y en la Instrucción Técnica de Seguridad de Conformidad con el ENS.

19. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política serán aprobados por el órgano superior competente que corresponda, de acuerdo con los artículos 11 y 12 del ENS. En nuestro caso es aprobada por el CEO mediante su firma.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas. La Política de Seguridad está notificada, comunicada y disponible para todo el personal de FRACTTAL.

20. REFERENCIAS

- Normativa de Seguridad: conjunto de políticas, normativas, procedimientos, registros y documentos disponibles en el repositorio documental del SGSI.
- Guías CCN-STIC del Centro Criptológico Nacional, en especial: CCN-STIC 805 (Política de Seguridad), CCN-STIC 801 (Responsabilidades y funciones), CCN-STIC 803 (Valoración de sistemas), CCN-STIC 804 (Medidas de implantación del ENS).

21. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR

Las revisiones y modificaciones de la presente Política las realizará el Comité de Seguridad de la Información, de acuerdo con el apartado 19.

En caso de cambios sustanciales o de los principios o responsabilidades designadas, el Comité propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por el CEO de la compañía, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.