tracasa instrumental

Fecha
05.06.2024

Política de Seguridad de la Información

Índice

1 Aprobación y entrada en vigor

Texto aprobado el día 5 de junio de 2024 por la Dirección de la empresa.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día 9 de noviembre de 2023 por la Dirección de la empresa.

Par la elaboración de esta Política, así como las futuras modificaciones que pueda experimentar, se ha seguido la documentación relativa al ENS y en especial la GUÍA DE SEGURIDAD (CCN-STIC-805) ESQUEMA NACIONAL DE SEGURIDAD: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

2 Principios rectores

Tracasa Instrumental enfoca la seguridad de la información como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación de la seguridad está presidida por este principio, que excluye en consecuencia cualquier actuación puntual o tratamiento coyuntural.

Tracasa Instrumental dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI) para alcanzar sus objetivos, certificado bajo el estándar internacional ISO 27000.

Este SGSI debe ser administrado con diligencia, tomando las medidas adecuadas para proteger a las empresas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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, uso previsto y valor 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 la empresa debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad y el estándar ISO 27000, 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.

La empresa debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La empresa debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 Prevención

Tracasa Instrumental debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, la empresa implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la empresa debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

Tracasa Instrumental se compromete a:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros organismos con los que guarde relación.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la empresa debe desarrollar y mantener planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3 Alcance

Esta política se aplica a Tracasa Instrumental y a todos los miembros de la organización, sin excepciones.

4 Misión de Tracasa Instrumental

Desarrollar conocimiento, personas y servicios innovadores, en colaboración con las administraciones públicas y con empresas privadas.

5 Marco normativo

El listado de las principales leyes, reglamentos y otra normativa a la que Tracasa Instrumental está sujeta es:

1. Empresa:

- Real Decreto Legislativo 1/2010, de 2 julio por el que se Aprueba el texto refundido de la ley de Sociedades de Capital.
- Ley Foral 13/2007, de 4 de Abril, de la Hacienda Pública de Navarra.
- Ley Foral 14/2007, de 4 de abril, del Patrimonio de Navarra
- Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público institucional foral
- Ley Foral 2/2018 de Contratos Públicos de Navarra
- Ley 15/2007, de 3 de julio, de Defensa de la Competencia.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones
- Ley Foral 11/2002 de 9 de Noviembre de Subvenciones
- Convenio Colectivo del Sector Oficinas y Despachos de Navarra
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores)

2. Seguridad de la Información:

- Artículo 18 de la Constitución Española
- Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 10/2021, de 9 de julio, de trabajo a distancia
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Reglamento (UE) n ° 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 y por la que se deroga la Directiva 1999/93/CE
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el 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 la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio. Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Instrucciones Técnicas de Seguridad (ITS) publicadas por el CCN.

3. Normativa por la ejecución de fondos MRR:

- Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.
- Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia
- Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.)
- Resolución 1/2022, de 12 de abril, de la Secretaria General de Fondos Europeos, por la que se establecen instrucciones a fin de clarificar la condición de entidad ejecutora, la designación de órganos responsables de medidas y órganos gestores de proyectos y subproyectos, en el marco del sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.
- Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.

6 Procedimientos de Seguridad

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto y que forman parte del SGSI de Tracasa Instrumental, principalmente:

- normas de seguridad: uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

- guías de seguridad: carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos
- procedimientos de seguridad: afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

6.1 Alta Dirección

- La Alta Dirección es responsable de que Tracasa Instrumental alcance sus objetivos a corto, medio y largo plazo.
- Debe respaldar explícita y notoriamente las actividades del SGSI en la organización.
- Expresa sus inquietudes al CSI a través del Responsable de Seguridad de Información (RSI).
- Aprueba la Política de Seguridad de Tracasa Instrumental.
- Decide sobre la aprobación de presupuestos presentados por el CSI.

6.2 Comité de Seguridad de la Información (CSI)

El CSI de Tracasa Instrumental tiene las siguientes funciones y responsabilidades:

- Coordinar todas las funciones de seguridad de la empresa
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Responsabilizarse de la elaboración de la Política de Seguridad de la Información, que será aprobada por la Alta Dirección.
- Aprobar las políticas de seguridad de las diferentes áreas.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad.
- Escuchar las inquietudes de la Alta Dirección y transmitirlas a los responsables de la empresa que tengan competencias en el ámbito de la seguridad. De estos últimos podrá recabar respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.
- Recabar del Responsable de Seguridad de la Información (CSO de acuerdo a la denominación del ENS) informes regulares del estado de seguridad de la organización y de los posibles incidentes.
- Coordinar y dar respuesta a las inquietudes transmitidas a través del CSO.
- Definir, dentro de la Política de Seguridad de la Información, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.

El CSI de Tracasa Instrumental está formado por los siguientes roles:

- Gerencia
- Responsable de la Información / Responsable del Servicio
- Responsable de Seguridad de la Información
- Responsable de Sistemas
- Dirección de Servicios Corporativos
- Responsable de Jurídico, Protección de Datos, Compliance y Seguridad física
- Responsable de Personas y Talento

El Secretario del CSI será el Responsable de Seguridad de la Información y tendrá las siguientes funciones en el ámbito del CSI:

- Convocar al CSI, recopilando la información pertinente.
- Recabar las inquietudes de la Dirección de la entidad y de las distintas áreas, incorporándolas al Orden del Día del CSI, para su examen y acciones pertinentes.
- Estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al CSI y proponiendo las medidas oportunas de adecuación al nuevo marco.
- Responsable de la toma de decisiones cotidianas entre dos reuniones del CSI. Estas decisiones darán respuesta a propuestas de las áreas, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

6.3 Roles: funciones y responsabilidades

Se concretan en este apartado las funciones y responsabilidades de los siguientes roles, tal y como establece el Esquema Nacional de Seguridad y habiéndose aplicado guía CCN-STIC 801 como modelo:

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
Responsable de la Información	ENS, art. 10	Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable. El ENS define "sistema de información" como: "Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir". (Anexo IV. Glosario).
Responsable del servicio	ENS, art. 10	Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.
	ENS, art. 39	Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
	ENS, art. 43	Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
Responsable de la Seguridad	ENS, art. 10	Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Deberá ser una persona física, jerárquicamente independiente del Responsable del Sistema. Nota: En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio).
	ENS, art. 15.3	Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios deseguridad cuenten con profesionales cualificadosy con unos niveles idóneos de gestión y madurezen los servicios prestados.
	ENS, art. 18	En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivelde seguridad determinados, aquellos que tengancertificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.
	ENS, arts. 27.3, 27.4 y 27.5	Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el Responsable de la Seguridad. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
	ENS, art. 28	La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilizaciónde estas infraestructuras y servicios comunes serán determinados por cada Administración.
	ENS, art. 34.6 y Anexo III	Los informes de autoevaluación y/o los informesde auditoría serán analizados por el Responsablede la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
Responsable del Sistema	ENS	Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de laSeguridad.
	La derivada de la aplicación dela Ley 40/2015	Su responsabilidad puede estar situada dentro dela organización (utilización de sistemas propios)o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.
	ENS, art. 34.6 y 34.7	Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
Administrador de la Seguridad del Sistema (ASS)	N/A	La persona designada figurará en la documentación de seguridad del Sistema de información, y sus funciones son las siguientes: La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. 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 de Información. La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
		actividad desarrollada en el sistema se ajusta a lo autorizado. La aplicación de los Procedimientos Operativos de Seguridad. Aprobar los cambios en la configuración vigente del Sistema de Información. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.  **Ilustración 2 - El ASS depende del Responsable del Sistema**

6.4 Responsable de Seguridad

El Responsable de la Seguridad (de la información) es la persona designada por la Dirección de la entidad, según el procedimiento descrito en su Política de Seguridad de la Información.

El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Además de ello, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).

Las dos funciones esenciales del Responsable de la Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Además de ello, cuando la figura del Responsable de la Seguridad del ENS coincide con la Entidad Responsable de Seguridad de la Información derivada de la Directiva NIS15, como es el caso de Tracasa Instrumental, podrá desplegar las siguientes funciones:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

6.5 Procedimiento de designación

El Responsable de Seguridad de la Información será nombrado por Gerencia a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.6 Resumen de funciones de cada rol

En la tabla se usan las siguientes abreviaturas:

CSI – Comité de Seguridad de la Información
RINFO – Responsable de la Información
RSERV – Responsable del Servicio
RSEG – Responsable de la Seguridad
RSIS – Responsable del Sistema
ASS– Administrador de la Seguridad del Sistema

tarea	responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba : Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG

Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

6.7 Nombramientos y jerarquía

La Dirección de Tracasa Instrumental, en cumplimiento de la guía CCN-STIC 801 en su apartado 10, nombra:

- al Responsable de la Información
- al Responsable del Servicio, si fuera distinto al Responsable de la Información
- al Responsable de la Seguridad, que debe reportar directamente a la Dirección y al Comité de Seguridad de la Información.
- al Responsable del Sistema, que, en materia de seguridad, debe reportar al Responsable de la Seguridad

6.8 Especificidades

1. Independencia entre el Responsable de Seguridad y el Responsable del Sistema

El Responsable de la Seguridad será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos y tal y como establece el artículo 13 del ENS.

2. Responsabilidades unificadas entre el Responsable de la Información y el Responsable del Servicio

La diferenciación entre ambos roles tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

En el caso de Tracasa Instrumental ambos roles están unificados en la figura del Director de Operaciones.

6.9 Resolución de conflictos

De conformidad con lo dispuesto en el artículo 3 de la Ley 40/2015, que señala que las Administraciones Públicas, sirviendo los intereses generales, desarrollarán su actividad con plena observancia de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.

7 Profesionalidad

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Tracasa Instrumental exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Tracasa Instrumental determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

8 Autorización y control de accesos

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

9 Protección de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la normativa aplicable relativa a la protección de las infraestructuras críticas.

10 Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan

certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, a través del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del CCN considerando, excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

11 Mínimo privilegio

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

12 Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

13 Protección de la información almacenada y en tránsito

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

14 Prevención ante otros sistemas de información interconectados

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad del ENS correspondiente.

15 Registro de la actividad y detección de código dañino

Tracasa Instrumental registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Tracasa Instrumental podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

16 Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

17 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el SGSI establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El CSI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

18 Datos de carácter personal

Tracasa Instrumental trata datos de carácter personal. Todos los sistemas de información de Tracasa Instrumental se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

19 Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Tracasa Instrumental recogidas en su SGSI.

Esta Política se desarrollará por medio de normativa de seguridad que afronte 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.

La normativa de seguridad estará disponible en la intranet: : Intranet de Tracasa Instrumental (tracasa.es) e impresa y custodiada en las oficinas de la empresa pública NASERTIC sitas en Calle Orcoyen, s/n, 31011 Pamplona, Navarra.

19.1 Ciclo de vida de la Política

Será misión del CSI 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 Seguridad y difundida para que la conozcan todas las partes afectadas.

20 Obligaciones del personal

Todos los miembros de Tracasa Instrumental tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del CSI disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de Tracasa Instrumental, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

21 Terceras partes

Cuando Tracasa Instrumental preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Tracasa Instrumental utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Firmado digitalmente por:
44624007M MARGARITA
GONZALEZ (R: B71280689)
Fecha y hora: 03.07.2024
09:06:56

Mar González Paredes
Directora General de Tracasa Instrumental

tracasa instrumental

Gobierno de Navarra / Nafarroako Gobernua

cpen

TÜVRheinland CERTIFICADO

Sistema de Gestión ISO/IEC 27001:2013

www.tuv.com ID 9108641606

AENOR

GESTIÓN AMBIENTAL

ISO 14001