1. INTRODUCCIÓN

Tempo Consultoría Estratégica S.L. (en adelante **TEMPO**) es una empresa de referencia en términos de calidad de servicio, profesionalidad y compromiso con nuestros clientes, comunicándonos con ellos de manera abierta, directa y sincera, favoreciendo una total integración de nuestra actividad con la de nuestros clientes a medio y largo plazo, estableciendo un claro compromiso de contribución a la mejora continua, desarrollo sostenible, y seguridad, proporcionando una elevada calidad de los servicios de consultoría entregados, otorgando una visión estratégica a largo plazo, respetando los preceptos sobre matera social, trabajo, medioambiente e igualdad.

Nuestra cultura compartida con todas las personas que forman parte de nuestra organización da soporte a nuestra filosofía de servicio:

- La profesionalidad, el compromiso, el rigor, el esfuerzo y la flexibilidad en el desarrollo de las funciones por parte de cada miembro de la organización.
- El trabajo en equipo, como fórmula que propicia la comunicación, la expresividad, la accesibilidad y la cohesión entre todos los miembros de la organización.
- El fomento de la creatividad, como forma de facilitar el desarrollo de una estética y estilos propios, y la innovación de los sistemas.
- La transparencia en el ejercicio de la actividad y la eficiencia económica, con el fin de conseguir la rentabilidad del negocio de nuestros clientes.

Tempo Consultoría Estratégica fue fundada en el 2003, y disponemos de una cartera con clientes internacionales, una capacidad de servicio sobre referenciales múltiples, ofreciendo una capacidad de adaptación en función de las capacidades de nuestros clientes, satisfaciendo plenamente las expectativas que generamos, haciendo de nuestra actividad un complemento de la suya.

TEMPO define como las bases de nuestra política empresarial son: Calidad, Liderazgo, Técnica y Servicio que unido a nuestro objetivo fundamental: Satisfacción completa de nuestros clientes, constituyen los elementos básicos de nuestra actividad empresarial, con un claro compromiso a la contribución y mejora del Desarrollo Sostenible, nuestras empresas adoptan una visión estratégica a largo plazo basada en la elevada calidad de los servicios prestados, en el respeto hacia los derechos fundamentales en materia social y de trabajo, el cumplimiento normativo penal, en una apuesta respetuosa hacia el medio ambiente, así como un compromiso de mantenimiento de la confidencialidad, integridad y disponibilidad de la información de la organización; de este modo, la calidad, el compromiso ambiental, la seguridad y salud en el trabajo, la seguridad de la información y el compliance penal se convierten en la piedra angular de nuestra visión.

La Dirección suscribe estos preceptos en su Política del Sistema Integrado de Gestión publicada en la web y comunicada a todas las partes interesadas.

Localización de TEMPO Consultoría Estratégica S.L.:

En la actualidad, TEMPO tiene su sede en:





DIRECCIÓN.
Av. de Monelos, 99, 1ºD, 15009 A Coruña, La Coruña

2. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN

La información es un recurso que, como el resto de los activos, tiene valor para **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.** y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se asegura un compromiso manifiesto de la Dirección de **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.** y de los directores de cada uno de los departamentos para la difusión, consolidación y cumplimiento de la presente política.

Esta Política se aplica en todo el ámbito de la organización, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Para determinar el alcance y la aplicabilidad del sistema de gestión, TEMPO CONSULTORÍA ESTRATÉGICA, S.L. ha tenido en cuenta:

- Las cuestiones externas e internas indicadas en 4.1 del MIG (Manual Integrado de Gestión)
- Los requisitos de las partes interesadas indicadas en el apartado 4.2 del MIG.
- Los resultados de la evaluación de riesgos penales indicada en el apartado 6.1 del MIG
- Los servicios de TEMPO CONSULTORÍA ESTRATÉGICA, S.L.

Siendo el alcance definido el indicado en el capítulo 4.3 del MIG, extraídos a este punto.

Los sistemas de información soportan los servicios de:

- Diseño, implantación, mantenimiento y auditoría de sistemas de gestión de la Calidad, Medio Ambiente, la Seguridad y Salud en el Trabajo, la Seguridad de la Información, Protección de los Datos de Carácter Personal, Esquema Nacional de Seguridad, Gestión de información de privacidad, Continuidad de Negocio, la Gestión de Servicios TI, TISAX (Trusted Information Security Assessment eXchange), Eficiencia Energética, Gestión de Riesgos, Gestión de Inteligencia Artificial, Seguridad en la Cadena de Suministro, Seguridad del Paciente, Seguridad Vial, Compliance, I+D+i, Responsabilidad Social, sostenibilidad y contribución a los ODS, Transportes de Pasajeros, Competencia de Laboratorios de Ensayo y Calibración, Cadena de Custodia FSC-PEFC, Q Calidad, Marcado CE de producto, Huella de carbono.
- Realización de Memorias de Sostenibilidad y Responsabilidad Social Corporativa e Informes no Financieros / información corporativa en materia de sostenibilidad; así como la prestación de servicios técnicos profesionales (asesoramiento fiscal y contable, preparación y elaboración de declaraciones y liquidaciones fiscales y contables, asesoramiento estratégico a dirección, elaboración de diagnósticos de competitividad y planes estratégicos).

de acuerdo a la categorización vigente.

3. LEGISLACIÓN DE REFERENCIA

TEMPO, mantiene un robusto control sobre la legislación de aplicación de seguridad de la información gracias al P-04 Control de Información Documentada, y al seguimiento de la normativa implantado, registrado y revisado anualmente en su "LISTA DOCUMENTOS EN VIGOR".

Las más importantes, y de las que hemos tomado mayor referencia en nuestros procesos de seguridad de la información son:

- ENS 311/22. Disposición 7191 del BOE Número 106 del 5 de mayo, 2022
- LOPDGDD 3/2018. Disposición 16673 del BOE Número 294 del 5 de diciembre, 2018.
- Ley 34/2002 de Servicios de la Sociedad de la Información y el Comercio Electrónico.
- ITS DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN BOE-A-2018-4573
- ITS DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD BOE-A-2016-10109
- ITS DE INFORME DEL ESTADO DE LA SEGURIDAD BOE-A-2016-10108
- ITS DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD BOE-A-2018-5370

La evaluación de riesgos sobre datos personales se ha tenido en cuenta para la valoración de las medidas de seguridad implantadas en el sistema.

4. PRESENTACIÓN DE PRINCIPIOS BÁSICOS

La Dirección de TEMPO, ampara, defiende y comunica los principios aquí presentados a toda la plantilla, los cuales tendrán consideración de fundamentos para la aplicación del Esquema Nacional de Seguridad. La organización velará por su protección y mantenimiento, garantizando así la funcionalidad del sistema y de sus competencias.

4.1. Seguridad como proceso Integral (Art. 6)

La aplicación del ENS estará presidida por este principio.
La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

4.2. Principio de Mínimo Privilegio. (Art. 20)

El principio de Mínimo Privilegio es la base sobre la que se sustenta la gestión de acceso a la información, asegurándonos que nuestros trabajadores pueden acceder a la información que necesitan, cuando la necesitan. Por ello la información se encuentra compartimentada garantizando que sólo aquellos a los que le es pertinente la información son capaces de alcanzarla y gestionarla.

4.3. Gestión de la seguridad basada en los riesgos. (Art. 7)

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos **(P-06 Identificación de Activos y Evaluación de Riesgos)** permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

4.4. Prevención, detección, respuesta y conservación. (Art. 8)

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de **seguridad (P-02 No Conformidades, Incidentes de seguridad y Acciones Correctivas).**

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

4.5. Existencia de líneas de defensa. (Art. 9)

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
b) Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica según las necesidades de la información, considerando todos sus soportes y cuando esta se transfiera o desplace. Asimismo, se monitorizarán y evaluarán las conexiones entre sistemas interconectados **(P-11 Gestión de Infraestructuras).**

4.6. Vigilancia continua y reevaluación periódica. (Art. 10)

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad o de sus componentes, si fuese necesario.

- P-01 Auditorías Internas.
- CG-01 Control Procesos
- P-08 Gestión de Continuidad y Disponibilidad.
- P-09 Gestión de la Capacidad
- MIG y Revisión por la Dirección

El **Responsable de Seguridad** será el encargado de realizar el adecuado control interno para evaluar la eficacia de los controles implementados y tener actualizados todos los procedimientos y procesos aplicados en la empresa ante posibles cambios de negocio o de requisitos de seguridad.
Para optimizar y mejorar de modo permanente el sistema de gestión de la seguridad de la información, al menos, se tendrán en cuenta las siguientes actividades:

- El registro y seguimiento de no conformidades y reclamaciones.
- El registro y seguimiento de las acciones correctivas.
- El registro y seguimiento de las acciones preventivas realizadas.
- Análisis periódico de las mejoras propuestas.

En cada ciclo del sistema se plantearán nuevos objetivos de mejora, planificándolos adecuadamente para poder realizar su correspondiente seguimiento.

Para ello, habrá dos tipos de actuaciones:

- Revisión anual del sistema.
- Revisión ocasional ante fallas importantes de seguridad que deban ser subsanadas de inmediato.

4.7. Diferenciación de responsabilidades. (Art. 11)

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos **(CG-01 Control de Procesos).**

4.7.1. Roles, responsabilidades y autoridades.

Se han definido las funciones y actividades que tienen incidencia sobre el ENS, y se establecen las responsabilidades, así como las interrelaciones entre las personas que las ejecutan. Esta información aparece documentada en el organigrama y en la definición de los puestos de trabajo, tal y como se establece en el CG-01 Control de Procesos. La asignación de estos responsables corre a cargo de la dirección de TEMPO, ratificándose la aceptación en documento firmado por los constituyentes o responsables.

A continuación, definiremos los puestos que el real decreto contempla para el Sistema de Seguridad de Información aplicados a TEMPO, explicando sus funciones, deberes y responsabilidades:

4.7.1.1. Responsable de la información

Este es una persona que ocupe un alto cargo en la Organización.

Es la persona a la que se deben comunicar las incidencias detectadas en la gestión de los datos (personales o no) sobre los que ostenta responsabilidad. El ENS le atribuye la potestad para establecer el “nivel de seguridad” de la información. Puede ser persona concreta u órgano colegiado según la estructura administrativa interna.

Su misión es velar por que se adopten las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de la información (incluidos los datos de carácter personal) tratada por los servicios y se evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Tendrá la responsabilidad última del uso que se haga de esta información y, por tanto, de su protección, al ser el responsable último de cualquier error o negligencia que lleve a un incidente de seguridad.

Establecerá los requisitos de la información en materia de seguridad (determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el anexo I del Esquema Nacional de Seguridad) aunque la

aprobación formal de los niveles corresponda al responsable de la información, este podrá pedir una propuesta del Responsable de Seguridad y conviene que escuche la opinión del Responsable de Sistema.

4.7.1.2. Responsable del servicio

Este tiene la potestad para establecer los requisitos del servicio en materia de seguridad, habitualmente coincide con responsables de Área o Departamento. También se podrá asignar este rol al Comité de Seguridad.

La prestación del servicio siempre debe atender a los requisitos de seguridad de la información que maneja y suele añadir requisitos de disponibilidad, accesibilidad e interoperabilidad.

El ENS le atribuye la responsabilidad última del uso que se haga de determinados servicios y por tanto de su protección.

Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del ENS.

Aunque la aprobación final de los niveles corresponda al Responsable del Servicio, podrá pedir una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, por lo que pueden heredar los requisitos de seguridad de esta, añadiendo requisitos de disponibilidad, así como otros como interoperabilidad, etc.

4.7.1.3. Responsable de seguridad

El responsable de la Seguridad tiene como responsabilidades:

- Velar por que se mantenga la seguridad de la información manejada y de los servicios prestados por los sistemas de información según lo establecido en la Política de Seguridad y lo acordado por el Comité de Seguridad.
- Promover la formación y concienciación en materia de seguridad. El ENS le otorga la potestad de supervisar el cumplimiento del propio ENS.
- Debe ser persona concreta (no puede ser órgano colegiado). Puede absorber las funciones del DPD siempre que posea la formación adecuada y se trate de una organización que por su tamaño no pueda justificar ambos roles (más información en el informe jurídico AEPD). Reportará directamente al Comité de Seguridad de la Información. Esta persona podrá convocar el Comité de Seguridad, recopilando la información pertinente.
- Supervisará (apoyándose técnicamente en el/los Administradores del Sistema) la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Organización. Promoverá la formación y concienciación dentro de su ámbito de responsabilidad. Recopilará los requisitos de seguridad de los Responsables de la Información y Servicio y ayudará a determinar con el Responsable del sistema la Categoría del Sistema.
- Coordinará la realización y actualización del Análisis de Riesgos.
- Debe elaborar y suscribir una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas de acuerdo al Anexo II de la ENS y del resultado del Análisis de Riesgos.
- Debe facilitar a los Responsables de Información y los Responsables de Servicio información sobre el nivel de riesgos residual esperado después de implementar las opciones de tratamiento seleccionadas

en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. Coordinará la realización y actualización de la documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por el órgano de gobierno y la alta dirección.
- Elaborará o coordinará y aprobará los procedimientos operativos de Seguridad de la Información.
- Debe facilitar periódicamente al Comité de Seguridad de la Información un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y el estado de la seguridad del sistema (en particular del nivel de riesgo residual a que está expuesto el sistema).
- Elaborará junto a los Responsables de Sistemas, Planes de mejora de la seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal de seguridad, que debe aprobar el Comité de Seguridad de la Información. Validará los Planes de continuidad de Sistemas que elabore el Responsable de Sistemas, si por la categoría de los sistemas a resultas del análisis de riesgos se requiere, que debe aprobar el Comité de Seguridad.
- Aprobará las directrices propuestas por los responsables de Sistemas para considerar los requisitos de Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, operación y cambios, sin menoscabo del Comité de Seguridad de la Información.

4.7.1.4. Responsable del sistema

- Supervisará las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobará los cambios en la configuración vigente del sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informará al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizará el estado de la seguridad del sistema.
- Implementará, gestionará y mantendrá las medidas de seguridad aplicables al Sistema de Información y asegurar que los controles técnicos de seguridad establecidos son cumplidos estrictamente.
- Asegurar la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentran habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida.
- Aplicar o asegurar que se aplican a los activos y recursos relacionados con los sistemas, tanto internos como externos, los procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos, en coordinación con el Responsable del Sistema y los Administradores de este. La gestión, configuración y actualización, en su caso, del hardware y software de en los que basan los mecanismos y servicios de seguridad del Sistema de Información.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevará a cabo el registro, contabilidad y gestión de los incidentes de seguridad en el/los sistemas bajo su responsabilidad.
- Ejecutará el plan de seguridad aprobado para aislar el incidente y evitar su propagación a elementos ajenos a la situación de riesgo.
- Tomará decisiones a corto plazo si la información se ha visto comprometida de alguna forma que pueda tener consecuencias graves (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).

- Asegurará la integridad y disponibilidad de los elementos críticos delo sistema si se han podido ver afectadas (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantendrá y recuperará la información almacenada por el Sistema y sus servicios asociados.
- Investigará el incidente: Determinará la manera, los medios, los motivos y el origen del incidente.

4.7.1.5. Responsable de la Gestión de Personal

Le corresponde implantar medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a este de su grado de implantación, eficacia e incidentes.

4.7.1.6. Comité de Seguridad

El personal asignado para formar parte del presente comité serán el Socio Director y el Socio Responsable de área de TI. Estas personas serán las encargadas de asegurar el correcto funcionamiento del Esquema Nacional de Seguridad, así como de la seguridad de TEMPO.

Las funciones del comité de seguridad se definen a continuación:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos. Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- 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 la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista 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. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- 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.

4.7.2. Resolución de conflictos.

Es potestad del Comité de Seguridad resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando a la Dirección aquellos casos en los que no tenga suficiente autoridad para decidir, o permanezca en equidad irresoluble.

5. GESTIÓN Y AUTORIZACIÓN DE PERMISOS

A continuación, se representa el cuadro de concesión de permisos y autorizaciones implantado por la Dirección de TEMPO, definiéndose quién autoriza y dónde se registra tales permisos:

	Requerimiento	Autoriza	Registros
– [org.4.1]	Utilización de instalaciones, habituales y alternativas.	CEO	Notificación empresarial en reunión de Responsables. Correo al personal Registro en Ticket para el cambio de infraestructuras
– [org.4.2]	Entrada de equipos en producción, en particular, equipos que involucren criptografía.	Comité de Seguridad	Gestión de *ticketing*
– [org.4.3]	Entrada de aplicaciones en producción.	Comité de Seguridad	Gestión de *ticketing* Reuniones
– [org.4.4]	Establecimiento de enlaces de comunicaciones con otros sistemas.	Comité de Seguridad	Gestión de *ticketing*
– [org.4.5]	Utilización de medios de comunicación, habituales y alternativos.	Comité de Seguridad	Solicitud por Teams, posible registro Gestión de *ticketing*
– [org.4.6]	Utilización de soportes de información.	Comité de Seguridad	Gestión de *ticketing, y* gestión de Dirección
– [org.4.7]	Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.	Dirección/Administración	Gestión de bienvenida, registro de onboarding. Todo el personal dispone de diferentes dispositivos bajo su custodia.
– [org.4.8]	Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.	Dirección	Control de acceso y/o contratación de servicio/Gestión de Adquisiciones

Toda autorización tendrá como último responsable a la Dirección de TEMPO, siendo esta la que ostenta la potestad de toda concesión dentro de TEMPO, siendo esta la otorga a los departamentos aquí representados la capacidad de gestionar las autorizaciones pertinentes para el normal flujo de información y recursos dentro de la organización.

6. REQUISITOS MÍNIMOS (Art. 12)

Los Requisitos mínimos solicitados por el Esquema Nacional de Seguridad se redactan a continuación, como expresión de su cumplimiento a través de toda la documentación del sistema y sus procesos:

6.1. Organización e implantación del proceso de seguridad. (Art. 13)

La Dirección de TEMPO ha establecido y segregado las responsabilidades necesarias para el ENS entre los Responsables actuales de la Organización segregando las responsabilidades para que ninguna caiga en conflicto, ratificándose estas decisiones en la aceptación de puesto.

En base a nuestra concienciación y profesionalidad de todo el personal podemos defender nuestra orientación y compromiso con la Seguridad de la Información.

6.2. Análisis y gestión de los Riesgos. (Art. 14)

La protección de los riesgos a la Seguridad de la Información es una parte de nuestro negocio, así mismo evaluamos los nuestros bajo un método probado y eficiente con más de 20 años de funcionamiento, actualizado para el Esquema Nacional de Seguridad, siempre en evolución. Nuestro Plan de Tratamiento de Riesgos resultante resultan siempre proporcionales y justificadas a nuestra organización y clientes.

6.3. Gestión de Personal. (Art. 15)

El activo más importante de TEMPO es mantenido por nuestro proceso de Recursos Humanos (presentado en el CG-01), y el cumplimiento de las medidas de seguridad por el Comité de Seguridad. Dirección presta atención a los requerimientos de profesionalidad requeridos por nuestros servicios.

6.4. Profesionalidad. (Art. 16)

La Dirección presta atención a los requerimientos de profesionalidad requeridos por nuestros servicios, representados en el Plan de Formación, y se evalúa de manera objetiva la de nuestros proveedores.

6.5. Autorización y control de los accesos. (Art. 17)

Las autorizaciones pasan por un proceso de control y gestión, desde la organización hasta el departamento SISTEMAS que crea las credenciales. Estas credenciales son auditadas durante toda su existencia.

6.6. Protección de las instalaciones. (Art. 18)

Los sistemas que dan soporte al servicio se encuentran en nuestras oficinas de TEMPO que se encuentran en Avenida Monelos 99-101, Microsoft (Azure) y en AWS (S3). Las instalaciones se encuentran protegidas de las amenazas presentadas en la evaluación de riesgos.

6.7. Adquisición de productos de seguridad y contratación de servicios de seguridad. (Art. 19)

Todo sistema será analizado a conformidad de los sistemas a implantar, validándose contra la guía CP-STIC 105, evaluándose:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

6.8. Mínimo privilegio. (Art. 20)

Referido en el punto 3.2 de este documento.

6.9. Integridad y actualización del sistema. (Art. 21)

Todo elemento dentro de nuestros sistemas es auditado, monitorizado y tenido en cuenta dentro de nuestro proceso de riesgos, siendo este sustentado por nuestras certificaciones ISO 27001, y nuestro robusto proceso PDCA (Plan, Do, Check, Act).

6.10. Protección de información almacenada y en tránsito. (Art. 22)

Nuestro almacenamiento ha sido protegido por sistemas de encriptación ampliamente validados, y mantenidos por nuestro equipo de sistemas.

Todo aquel disco que salga, tanto de nuestra infraestructura como de nuestros clientes, será protegido por nuestro procedimiento de cadena de custodia, otorgando la máxima protección a los Datos.

6.11. Prevención ante otros sistemas de información interconectados. (Art. 23)

Toda conexión es monitorizada por nuestros sistemas, las VPN solo las pueden configurar el personal habilitado para ello. Antes de validar una conexión se efectuará un análisis de los protocolos utilizados y de las medidas de seguridad interpuestas.

6.12. Registro de actividad y detección de código dañino. (Art. 24)

Los sistemas interpuestos prestan las mayores garantías del mercado en cuanto a protección y monitorización disponibles, encontrándose redundado para la máxima exactitud, prontitud de detección, y resiliencia de los sistemas.

Nuestro cumplimiento de la LOPDyGDD se encuentra asegurado por nuestro Responsable de Seguridad.

Toda esta monitorización se refleja en nuestro sistema de incidencias, y en la ardua labor de los responsables de TEMPO.

6.13. Incidentes de seguridad. (Art. 25)

Las incidencias de seguridad son gestionadas por SISTEMAS, con supervisión de la dirección, bajo nuestros procedimientos de gestión de incidentes, reforzados por nuestro desarrollo de la Continuidad de TI de TEMPO, desarrollado desde hace años, y en continua evolución y mejora.

6.14. Continuidad de la actividad. (Art. 26)

La protección de los registros y los DATOS es crítica para TEMPO, por ello se desarrollan y mejoran los procedimientos de Copias de Seguridad y Continuidad, monitorizando la realización de estos en tiempo real.

6.15. Mejora continua del proceso de seguridad. (Art. 27)

Como mínimo una vez al año se realiza una revisión del sistema por la dirección, para evidenciar el continuo despliegue y rendimiento de recursos de protección de la Información amparados en el Proceso de mejora continúa provisto por nuestras certificaciones.

6.16. Cumplimiento de requisitos Mínimos. (Art. 28)

Para dar cumplimiento a los requisitos mínimos establecidos en el real decreto 311/22 del 3 de mayo, esta política es presentada al personal de la organización y a aquellas partes interesadas competentes, siendo de obligado cumplimiento en el ejercicio de sus funciones al personal de TEMPO, especialmente al personal designado al cargo de su mantenimiento, presentando las bases para este cumplimiento en la Declaración de aplicabilidad del ENS, recogiendo todos los puntos del Anexo II del real decreto.

7. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

TEMPO ha establecido una serie de índices y mediciones con respecto al cumplimiento de los controles del Anexo II del ENS, los cuales se reflejan en el SOA, además de una serie de indicadores con el fin de evaluar la Seguridad en los procesos de la organización, y se realiza la presentación del Informe INÉS anualmente.

7.1. Grado de implementación de una medida de seguridad

Atendiendo al estado de implementación en que se encuentre cada una de las medidas de seguridad del anexo II del ENS, se pueden considerar como 'no implementadas', 'en proceso de implementación' o 'implementadas'.

En base a ello, se ha establecido una clasificación, con mayor nivel de detalle, referida al grado de implementación de cada una de las medidas de seguridad, que se muestra en forma de tabla a continuación:

Estado de Implementación	Grado de implementación	Descripción
No implementada 	G0	**Medida de seguridad pendiente de implementación.** En el grado G0 de implementación, la medida de seguridad no está siendo aplicada en este momento y quizá ni siquiera se contempla que lo sea en un futuro; No obstante, sí que debería aplicarse según la declaración de aplicabilidad del sistema o según el anexo II del ENS y la categoría, siempre
En proceso de implementación	G1	**Medida de seguridad con implementación iniciada.** En el grado G1 de implementación, la medida de seguridad como máximo existe a nivel de piloto o prototipo y, en el mejor de los casos, se han planificado y/o iniciado recientemente los trabajos necesarios para su implementación en producción.
		Medida de seguridad en implementación. En el grado G1 de implementación, la medida de seguridad está implementada en su parte material, pero la eficacia de la medida depende de la capacidad y buena voluntad de las personas, entre otras razones porque no está documentada (parte formal). Tampoco puede considerarse conocida por todos los interesados, al no haber directrices para ello.
Implementada	G2	**Medida de seguridad implementada.** En el grado G2 de implementación, la medida de seguridad está definida de forma documentada y, si corresponde, lleva procesos asociados y métricas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante posibles incidencias. Se ejerce un mantenimiento regular sobre la medida. *NOTA: Parte de la documentación puede estar embebida en determinada herramienta, por lo que dicha documentación puede referenciarla, o reproducirla, según aconseje cada caso particular y refrende el auditor.*
		Medida de seguridad medible y gestionable. En el grado G2 de implementación, se dispone de métricas e indicadores para conocer el desempeño (eficacia y eficiencia) de la medida, lo que posibilita gestionarla. *NOTA: En el grado G2 de madurez, el funcionamiento de las principales medidas de seguridad y los procesos asociados está bajo control, pudiéndose ajustar en función de las desviaciones observadas en los indicadores.*
		Medida de seguridad en ciclo de mejora continua. El grado G2 de implementación se centra en mantener la mejora continua de la medida de seguridad y los procesos asociados. Se alcanza cuando se rectifica y mejora la efectividad de la medida de seguridad con la suficiente continuidad y en base a las métricas e indicadores recopilados.

7.2. Valoración de la implantación de las medidas de seguridad

El modelo de madurez de capacidad (Capability Maturity Model, CMM) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

L0-Inexistente. (0%)

No existe un proceso que soporte el servicio requerido.

L1 - Inicial. Ad hoc. (20%)

La organización en este nivel no dispone de un ambiente estable para la prestación del servicio requerido.

Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

L2-Reproducible, pero intuitivo. (40%)

En este nivel la organización dispone de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

L3-Proceso definido. (60%)

Además de una buena gestión, a este nivel la organización dispone de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

L4-Gestionado y medible. (80%)

Se caracteriza porque la organización dispone de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

L5 - Optimizado. (100%)

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

Los Índices calculados, y representados en el SOA son el Índice de Madurez, y el Índice de Cumplimiento.

8. DOCUMENTACIÓN DE SEGURIDAD IMPLANTADA

TEMPO desarrolla y mantiene la documentación que da soporte al sistema, según se documenta en el P-02 Control de Documentación y los Registros, publicándose estos documentos en la intranet, concediendo acceso a aquellas personas que la organización considera están afectadas. Existe un listado de documentación en vigor, en el que se recogen las políticas aplicadas en el sistema, sometiéndola a un proceso controlado de distribución interna, que asegura la disponibilidad de la última versión actualizada en aquellos puntos donde ha de utilizarse.

Para evitar la pérdida, robo o transferencia no autorizada de la propiedad intelectual o información clasificada por TEMPO CONSULTORÍA ESTRATÉGICA, S.L., se seguirán las reglas principales siguientes:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- La firma por parte de todos los usuarios de un compromiso de confidencialidad.
- El seguimiento de todos los controles para el acceso, manejo, reproducción de dicha información.
- La monitorización de estos controles.
- El seguimiento de una política de puesto de trabajo despejado de papeles con información relevante y bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso, para asegurar la protección de información sensible.

Para garantizar que se realiza una protección eficaz, el RSEG impulsará la realización de un Inventario de Activos. Este proceso es un aspecto muy importante de la Gestión de Riesgos, ya que permite identificar el valor e importancia relativa a cada activo. Este inventario, se puede dividir según los activos asociados con los Sistemas de Información.

Los activos de información serán clasificados de acuerdo con la siguiente escala:

- **Confidencial:** Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias negativas para la organización

- **Uso Interno:** Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.

- **Público:** Información sin ninguna restricción de acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización

Tanto la autorización de acceso como la transmisión de la información confidencial por cualquier medio necesitan la aprobación expresa del responsable del activo. Siempre que sea factible, se enviará en archivo comprimido encriptado.

La destrucción de la información la realizará el responsable del activo siguiendo las siguientes pautas: formateo del equipo en el que se encuentra la información con el sistema operativo original, eliminación del

disco mediante métodos físicos (taladro), eliminación del papel mediante destructora y/o envío a empresa de destrucción confidencial.

La información confidencialidad en soportes electrónicos se etiquetará mediante una etiqueta de color blanco rectangular.

9. POLITICA DE USO ACEPTABLE DE LOS RECURSOS.

Las siguientes actividades están, en general, prohibidas. Los empleados pueden estar excluidos de esta prohibición temporalmente para la realización legítima de las responsabilidades de su trabajo (por ejemplo, administradores de sistemas pueden tener la necesidad de impedir el acceso a la red a un ordenador que se considera está provocando problemas, ha sido comprometido, ...).

En ninguna circunstancia, ningún empleado de **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.**, está autorizado para realizar alguna actividad ilegal (bajo cualquier legislación de cualquier ámbito sea este local, regional, nacional o internacional) con los recursos que la empresa pone a su disposición.

La siguiente lista no pretende ser exhaustiva, sino que intenta servir de guía de actividades que caen dentro de la categoría de uso no aceptable.

Actividades de Red y/o Sistemas:

- Violaciones de los derechos de cualquier persona o compañía protegidos por copyright, patente o cualquier tipo de propiedad intelectual, legislación y/o regulación existente, incluyendo (y sin limitarse sólo a esto) la instalación y/o distribución de software pirata o no licenciado para su uso por parte de **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.**
- Copia no autorizada, incluyendo fotocopia, digitalización... y posterior distribución de cualquier documento (revistas, libros, música...) o fuente con copyright.
- Introducción de programas, scripts o cualquier tipo de software malicioso en los servidores, ordenadores, dispositivos de red... (virus, gusanos, Trojan horses, e-mail bombs, etc.).
- Revelar la contraseña a otros. Esto incluye familiares y cualquier otra personal que pueda acceder desde cualquier ubicación externa a la empresa.
- Utilizar los medios que **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.** pone a su disposición para conseguir y/o transmitir material que viola las leyes de acoso sexual o abuso en el trabajo de cualquier tipo.
- Realizar ofertas fraudulentas de productos, artículos o servicios.
- Provocar problemas o pérdidas en el nivel de seguridad y/o caídas en las comunicaciones. Por problemas de seguridad también se entiende el acceso a información que no está dirigida a otros, utilizar cuentas para las que no se está autorizado (aunque se conozcan sus credenciales), acceder a ordenadores a los que no se tiene autorización, interceptar cualquier tipo de información de otros (especialmente claves), caídas o mermas de las comunicaciones incluyen actividades como capturas de

tráfico, ping floods, spoofing, ataques de denegación de servicio (sea esta parcial o total), falsear información de routing, port or security scanning, etc.

- Utilizar programas, scripts, comandos… o enviar mensajes de cualquier tipo con la intención de interferir o deshabilitar una sesión de un usuario en cualquier sentido, localmente o vía Internet, intranet, extranet.
- Proporcionar información o listas de los empleados de **TEMPO CONSULTORÍA ESTRATÉGICA, S.L.** a cualquier grupo externo a la empresa.

Actividades de comunicaciones o correo electrónico:

- Enviar mensajes de correo no solicitados, incluyendo "junk email" (varios correos casi idénticos enviados a múltiples destinos) o cualquier otro material publicitario a personas que no han solicitado dichos mensajes.
- Cualquier forma de acoso vía correo electrónico, teléfono, SMS… bien sea por el estilo del lenguaje, la frecuencia o el tamaño de los mensajes.
- Uso no autorizado o manipulación de la información de las cabeceras del correo.
- Solicitar correos de cualquier otra fuente distinta al destinatario con la intención de recopilar respuestas.
- Crear o reenviar "cartas en cadena", utilizar esquemas piramidales u otros sistemas similares.
- Envío de correos iguales o similares a grandes cantidades de grupos (listas de distribución, redes sociales, usenet newsgroups…).

10. APROBACIÓN

Por la presente se aprueba y se difunde la presente política en A Coruña, a fecha 30 de junio de 2026.

Ricardo Ulises Sobral Pujades
Dirección / Resp. Seguridad

Daniel Vázquez García
Dirección / Resp. Servicios

11. CONTROL DE CAMBIOS Y MODIFICACIONES

Edición	Fecha	Naturaleza del Cambio
00	01/03/2021	REINICIO DOCUMENTAL
01	24/11/2023	CAMBIO DE IMAGEN CORPORATIVA Y FORMATO
02	30/06/2026	INTEGRACIÓN ENS