POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

[POL-01]

cibernos®

EVOLUCIÓN DEL DOCUMENTO

Versión	Fecha	Autor	Comentarios
Preliminar	15-09-22	Miguel Alonso García	
2.0	18-01-2024	Ángel Ordieres	Como resultado de una no conformidad en auditoria de 2024 se añade al documento explícitamente: - Marco normativo (incluido marco normativo ENS) - Se añaden roles del ENS y funcionalidades. - Se añade composición del CSI
3.0	03-02-2026	Ángel Ordieres	Debido a la baja de larga duración del RS se nombra temporalmente al RI como RS

REVISIÓN DEL DOCUMENTO

Versión	Fecha	Nombre	Comentarios
1.0	19-09-2022	Comité de Seguridad	Primera versión
2.0	19-02-2024	Responsable de Seguridad	Notificada en reunión interna al Comité de Seguridad.
3.0	03-02-2026	Comité de Seguridad	Notificada en reunión interna al Comité de Seguridad

APROBACIÓN DEL DOCUMENTO

Versión	Fecha	Nombre	Comentarios
1.0	19-09-2022	Comité de Seguridad	
2.0	06/03/2024	Comité de Seguridad	
3.0	03/02/2026	Comité de Seguridad	

ÍNDICE

1. INTRODUCCIÓN 4

1. REFERENCIAS Y ANEXOS 4

2. PREVENCIÓN 5

3. DETECCIÓN 5

4. RESPUESTA 6

5. RECUPERACIÓN 6

6. ALCANCE 6

7. MISIÓN 6

8. MARCO NORMATIVO 8

9. NOMBRAMIENTOS Y ORGANIZACIÓN DE RESPONSABILIDADES 10

10.2 ROLES: FUNCIONES Y RESPONSABILIDADES 10
10.3 PROCEDIMIENTOS DE DESIGNACIÓN 16
10.4 DATOS DE CARÁCTER PERSONAL 16

10. CLASIFICACIÓN DE LA INFORMACIÓN 17

11. GESTIÓN DE RIESGOS 17

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 17

13. OBLIGACONES DEL PERSONAL 18

14. TERCERAS PARTES 18

1. INTRODUCCIÓN

Cibernos Consulting S.A depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados. Los diferentes departamentos deben 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. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el ENS.

1. REFERENCIAS Y ANEXOS

La implantación de este procedimiento requiere la consideración de la siguiente documentación:

- Política de Seguridad de la Información.
- Normativa de Seguridad.
- UNE-ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos.

- UNE-ISO/IEC 27002 Código de Prácticas para los Controles de la Seguridad de la Información.
- Documentos y guías del Centro Criptológico Nacional (CCN-STIC) referidos al ENS.

2. PREVENCIÓN

Los departamentos deben 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 los departamentos deben implementar 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, los departamentos deben:

- 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.

3. 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.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. 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.

4. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- 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).

5. RECUPERACIÓN

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

6. ALCANCE

Esta política se aplica a todos los sistemas TIC de Cibernos Consulting y a todos los miembros de la organización, sin excepciones.

7. MISIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, Cibernos Consulting, está altamente comprometido con mantener la Promoción de proyectos de investigación, desarrollo tecnológico e innovación, en un entorno de calidad, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada.

En consecuencia, a lo anterior, Cibernos Consulting, define los siguientes principios de aplicación para tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

La dirección de Cibernos Consulting, entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de los servicios de la organización y, por tanto, soporta los siguientes objetivos y principios:

I. Implementar el valor de la Seguridad de la Información en el conjunto de la Organización.
II. Contribuir, todas y cada una de las personas de Cibernos Consulting, a la protección de la Seguridad de la Información.
III. Preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información, con el objetivo de garantizar que se cumplan los requisitos legales, normativos, y de nuestros clientes, relativos a la seguridad de la información; y de forma específica en lo que respecta a datos de carácter personal:

   a. los datos serán tratados de manera lícita, leal y transparente en relación con el interesado (Licitud, lealtad y transparencia).
   b. Serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (Limitación de la finalidad)
   c. Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (Minimización de datos).
   d. Los datos deberán ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (Exactitud).
   e. Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (Limitación del plazo de conservación)
   f. Tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (Integridad y confidencialidad).

IV. Proteger los activos de la información de Cibernos Consulting de amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la continuidad del servicio ofrecido a nuestros clientes y la seguridad de la información.

V. Establecer un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por Cibernos Consulting.

VI. Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.

VII. Asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

VIII. Extender nuestro compromiso con la seguridad de la información a nuestro personal trabajador y proveedores.

IX. Mejorar continuamente la seguridad mediante el establecimiento y seguimiento periódico de objetivos de seguridad de la información.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

De igual forma, para gestionar los riesgos que afronta Cibernos Consulting se establece un procedimiento de evaluación de riesgos formalmente definido. Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección Ejecutiva de Cibernos Consulting.

8. MARCO NORMATIVO

La gerencia de Cibernos Consulting se asegura de que la documentación de origen externo que resulta de interés para el funcionamiento de la empresa es conocida por los empleados de la empresa que lo necesitan y es mantenida actualizada y disponible en todo momento.

Para ello se utilizan los medios definidos en este documento y los procedimientos que lo desarrollan.

En cuanto a normas aplicadas para formalizar los diferentes procedimientos de Seguridad establecidos se han seguido los criterios de las siguientes normas internacionales:

- Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. UNE-ISO/IEC 27001
- Tecnología de la información. Técnicas de seguridad. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. UNE-ISO/IEC 27002
- Exigencias de partes interesadas
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- LOPD y Garantías de los Derechos Digitales 03/2018
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 10/2021, de 09/07/2021, de trabajo a distancia, (BOE, Nº 164 de 10/07/2021) .

De forma adicional se crea el **Registro Normativa aplicable** para nutrir de toda la información, enlaces de interés e información relacionada con Normativa aplicada.

9. NOMBRAMIENTOS Y ORGANIZACIÓN DE RESPONSABILIDADES

La dirección de Cibernos Consulting se encarga de realizar unos nombramientos para designar los roles y responsabilidades, así como los comités necesarios, para velar por el cumplimiento de esta política. Esta documentación estará accesible para todas las partes interesadas y el personal interno a la organización.

10.2 Roles: funciones y responsabilidades

En el documento interno **REG-01 Roles y responsabilidades Cibernos Consulting** se recogen con detalle todos los roles y responsabilidades de la organización.

Resumimos los roles del SGSI:

RSER	Responsable del Servicio	C. C. L.
RINF	Responsable de la Información	Á. O. R.
RSEG	Responsable de Seguridad	Á. O. R.
RSIS	Responsable de Sistemas	M. G. R.
RPD	Responsable de Protección de Datos	Á. O. R.
RD	Responsable de Desarrollo	C. C. L.
RSIS	Responsable del Sistema (ENS)	C. C. L.
CSI	Comité de Seguridad de la Información	CC, AO, RT

POC	Punto de Control	Responsable de Seguridad

Se definen las funciones de cada rol:

Responsable de la información	Velar por el buen uso de la información y, por tanto, de su protección.
	Establecer los requisitos de la información en materia de seguridad.
	Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.
Responsable del servicio	Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
	Determinar los niveles de seguridad del servicio, de acuerdo con el Responsable de Seguridad y el Responsable del Sistema.
	Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
Responsable de seguridad	Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad y de la Norma UNE-ISO/IEC 27001.
	Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
	Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.
	Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
	Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas (ISO 27001 y ENS), en colaboración con el Responsable de Sistemas.
	Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.
	Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
	Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.
	Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
	Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
	Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.

	Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
	Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.
	Responsable de la ejecución directa o delegada de las decisiones de la Dirección, se reunirá con esta y con el Responsable del Sistema, al menos con una frecuencia anual, para asegurar la estrategia.
Responsable de protección de datos	Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación al RGPD y otras disposiciones de protección de datos.
	Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
	Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
	Cooperar con la autoridad de control;
	Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
Responsable del sistema	Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
	Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
	Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
	Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
	Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
	Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
	Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
	Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.

	Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
	Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
	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 de los sistemas de información.
	La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado
	La aplicación de los procedimientos operativos de seguridad.
	Aplicar los cambios de configuración del sistema de información.
	Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como 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 respectivos Responsables 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.
Responsable de Sistemas	Administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.

Responsable de Desarrollo	Programar / codificar las instrucciones necesarias que requiera según el diseño técnico y funcional recibido. Realizar pruebas de forma independiente los programas realizados . Escalar dudas o posibles discrepancias del diseño recibido al Project Manager . Resolver las incidencias técnicas que puedan presentar los programas, bien cuando ya están en producción como en las fases de pruebas . Puede colaborar en la elaboración de ciertas documentaciones, manuales, …. Formación a clientes . Estar pendiente y escalar rápidamente las posibles desviaciones en plazo/esfuerzos estimados para la realización de sus tareas, denunciando complejidades/PROBLEMAS no tenidos en cuenta o minusvalorados . Realizar y asumir, en su caso, las tareas de naturaleza análoga a las descritas, siempre que surjan como necesarias para la óptima consecución de los objetivos consustanciales al puesto, o sean asignadas al titular por sus mandos inmediatos o Responsabilidad en cuanto al producto entregado y al seguimiento de las normas de desarrollo, documentación, nomenclatura, … Estar siempre alerta para la recogida de nuevas necesidades en los clientes o Imputar tiempos a las herramientas de gestión y porcentaje de avance o Realizar y asumir, en su caso, las tareas de naturaleza análoga a las descritas, siempre que surjan como necesarias para la óptima consecución de los objetivos consustanciales al puesto, o sean asignadas al titular por sus mandos inmediatos. Conocer las políticas de la organización. Cumplir con las responsabilidades designadas en la protección de datos, las políticas aprobadas por la organización, mantener la confidencialidad en el desarrollo de sus tareas profesionales y de aquellas recogidas en el sistema de gestión de la organización o normativas aplicables
POC	Canalizar y Supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El Comité de Seguridad reportará a la organización y estará formado por:

- Presidente (el cargo de presidente lo ocupa un cargo con responsabilidad o cargo político para asegurar que las decisiones que se tomen se lleven a cabo): R. T. G.
- Secretario: Á. O. R.
- Vocales:
    - [RSIS-ENS]: C. C. L.
    - [RSEG]: Á. O. R.
    - [RINF / RPD]: Á. O. R.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando 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 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.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

El Comité se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

10.3 Procedimientos de designación

El responsable de Seguridad de la Información será nombrado por Dirección a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante. El Departamento responsable de un servicio que se preste electrónicamente, designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

10.4 Datos de carácter personal

Cibernos Consulting trata datos de carácter personal. El OneDrive corporativo (ubicado en la UE), al que tendrán acceso solo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de Cibernos Consulting se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

10. CLASIFICACIÓN DE LA INFORMACIÓN

Cibernos Consulting cuenta con un sistema interno de clasificación de información en función de su criticidad. Aquella información sensible con un nivel de criticidad relevante es cifrada y tratada antes de ser enviada o salir de la organización. Este sistema esta descrito y documentado en el sistema interno de la organización.

11. 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 Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

A causa de la protección de datos personales puede ser necesario aumentar las medidas propuestas por el propio ENS.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afrontará aspectos específicos en la operativa de los usuarios de IT de la organización. La normativa de seguridad estará a disposición de

todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

El Comité de Seguridad de la Información aprueba la utilización de SharePoint como repositorio de gestión documental y servirá de gestión de los controles del ENS.

La normativa de seguridad estará disponible en la página principal del repositorio de datos "SharePoint" de la empresa y disponible en la intranet corporativa alojada en el servidor interno principal de la empresa.

13. OBLIGACONES DEL PERSONAL

Todos los miembros de Cibernos Consulting tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados. Todos los miembros de Cibernos Consulting atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, 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.

14. TERCERAS PARTES

Cuando Cibernos Consulting 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 Cibernos Consulting 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. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. 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.

ORDIERES REGATO, ANGEL LUIS (FIRMA)

Firmado digitalmente por ORDIERES REGATO, ANGEL LUIS (FIRMA)
Fecha: 2026.02.04 13:05:49 +01'00'

CONTRERAS LLINARES CARLOS - 48953243C

Firmado digitalmente por CONTRERAS LLINARES CARLOS - 48953243C
Fecha: 2026.02.04 13:54:53 +01'00'

TOLEDO GARCIA ROGELIO - 02893271D

Firmado digitalmente por TOLEDO GARCIA ROGELIO - 02893271D
Fecha: 2026.02.05 07:59:12 +01'00'