TECNOVA INGENIERÍA Y SISTEMAS, S.A.

MARCO ORGANIZATIVO:
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (or.1)

ESQUEMA NACIONAL DE SEGURIDAD			
Política de seguridad			POL - 1
V 1.0	PÚBLICO ☒	INTERNO ☐	CONFIDENCIAL ☐
			NÚMERO DE PÁGINAS: 30

ÍNDICE

POLÍTICA DE SEGURIDAD

ESQUEMA NACIONAL DE SEGURIDAD

D./ Dña. CÉSAR LANZA SUÁREZ, mayor de edad, con DNI 09703316F, actuando en nombre y representación de TECNOVA INGENIERÍA Y SISTEMAS, S.A., provista de CIF A79007134, y con domicilio a efectos de notificaciones en CALLE PRÍNCIPE DE VERGARA, 33, 2º IZQUIERDA, 28001 – MADRID (Madrid).

Esta Política de Seguridad de la información es efectiva desde la fecha de aprobación 02-06-2026, y hasta que esta sea reemplazada por una nueva Política de seguridad.

IDENTIFICACIÓN CONTACTO:

- **Denominación social:** TECNOVA INGENIERÍA Y SISTEMAS, S.A.
- **CIF/NIF:** A79007134
- **Actividad:** DESARROLLO DE SOFTWARE Y CONSULTORÍA INFORMÁTICA
- **Teléfono de contacto:** 912091065 / 678505887
- **Domicilio social:** CALLE PRÍNCIPE DE VERGARA, 33, 2º IZQUIERDA, 28001 – MADRID (Madrid)
- **Domicilio a efecto de notificaciones:** CALLE PRÍNCIPE DE VERGARA, 33, 2º IZQUIERDA, 28001 – MADRID (Madrid)
- **Dirección electrónica de contacto:** javier.santos@tecnova.es
- **Página web (URL):** www.tecnova.es

CONTROL DE REVISIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO
1.0 14/02/2026	Versión inicial	Javier Santos

1.- OBJETO

TECNOVA INGENIERÍA Y SISTEMAS, S.A. (en adelante, la entidad) depende de los sistemas TIC (Tecnología de Información y Comunicaciones) para alcanzar sus objetivos.

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 (ENS en adelante), 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 al artículo 7 del ENS.

2.- ALCANCE

La presente política de seguridad ha sido desarrollada e implementada bajo la normativa exigida. Esta política se aplica a todos los sistemas TIC recogidos en el documento, que forma parte de su sistema generado para documentar las medidas mínimas de seguridad exigidas por el ENS, bajo la denominación “Declaración de Alcance”.

3.- LEGISLACIÓN Y NORMATIVA APLICABLE

- Ley 34/ 2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 39/2015 de 1 de octubre, de administrativo común de las administraciones públicas.
- Ley 40/2015 de 1 de octubre, de régimen jurídico del sector público.
- 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.
- Real Decreto 203/ 2021, de 30 de marzo, por el que se aprueba el reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016.
- GUÍAS CCN-STIC.
- UNE - ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- UNE - ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
- UNE-EN-ISO 9001:2015 sistemas de gestión de la calidad.

4.- VIGENCIA

La presente Política de Seguridad ha sido aprobada por la dirección de la entidad, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la entidad pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la entidad.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Política de Seguridad.

5.- PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de activos de información.

La entidad depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos.

Dichos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad 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 a los incidentes.

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

> *El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos: a) Seguridad como proceso integral. b) Gestión de la seguridad basada en los riesgos. c) Prevención, detección, respuesta y conservación. d) Existencia de líneas de defensa. e) Vigilancia continua. f) Reevaluación periódica. g) Diferenciación de responsabilidades.*

De este modo, las amenazas no se materializarán y en caso de que ocurriese la idea principal es que no afecten gravemente a la información que maneja, o los servicios que se prestan.

Se desarrollarán, al menos los siguientes objetivos:

> a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

5.1.- Prevención

La entidad 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 los departamentos o áreas 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, 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.

5.2.- 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 10 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

> "*La vigilancia continua permitirá la detección de actividades o comportamiento anómalos y su oportuna respuesta. 2.La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. 3.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, si fuese necesario."

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

"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. 2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica."

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.

5.3.- Respuesta

Los departamentos o áreas 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).

5.4.- Recuperación

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

6.- ORGANIZACIÓN DE LA SEGURIDAD

6.1.- Definición de roles

La implantación de la Política de Seguridad en la entidad requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos de seguridad, requisitos del sistema y requisitos del servicio.

Es por ello que, la Política de Seguridad, según se detalla en el ANEXO II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su sección 3.1, deberá identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros.

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección será responsable de organizar las funciones y responsabilidades, la política del Organismo, y por último de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

6.2.- Comité de Seguridad: Funciones y Responsabilidades

La seguridad de la Información es una responsabilidad organizativa. En consecuencia, se promueve la composición de un Comité de Seguridad de la Información, con el interés de establecer una vía definida y de apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por cada una de las figuras, que en este epígrafe se detallan, de responsables y por un presidente que será responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

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

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
  - Principales incidencias en la Seguridad de la Información.
  - Elaboración y actualización de planes de continuidad.
  - Cumplimiento y difusión de las Políticas de Seguridad.

Para documentar la composición del Comité de Seguridad se utiliza el documento adjunto a la presente Política de seguridad como ANEXO I

6.3.- Roles y Responsabilidades

Los diferentes roles de seguridad de la información se limitan a una jerarquía simple: el Comité de Seguridad de la Información y los diferentes Responsables, donde rige el principio básico de diferenciación de responsabilidades tal y como se establece en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Diferenciando así el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

Por su parte, el Delegado de Protección de Datos debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad.

En concreto, la organización debe designar los siguientes roles:

RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información de la entidad establecerá los requisitos, en materia de seguridad, de la información gestionada.

Se deberá tener en cuenta que, si dicha información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la normativa de protección de datos.

Las obligaciones del Responsable de la Información son:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer en los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información en la entidad.

Se ha designado como Responsable de la Información a la persona recogida en el documento adjunto a la presente Política como **ANEXO II**.

Se adjunta en la presente Política como **ANEXO IV** comunicado formal para la designación de Responsables de la Información, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLE DEL SISTEMA

El Responsable del Sistema asegurará la ejecución de medidas para protección de los activos y de los servicios de los sistemas de información que soportan la actividad de la entidad.

Las obligaciones del Responsable del Sistema son:

- Desarrollar, operar y mantener el Sistema de Información la entidad durante el ciclo de vida, especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad de la entidad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de la entidad conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en la entidad.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. o Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

Se ha designado como Responsable del Sistema a la persona recogida en el documento adjunto a la presente Política como **ANEXO II**.

Se adjunta en la presente Política como **ANEXO VI** comunicado formal para la designación del Responsable de Seguridad, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLE DE SEGURIDAD

El Responsable de la Seguridad de la Información de la entidad será el responsable de la coordinación y verificación de cumplimiento de los requisitos de seguridad de la información.

Las obligaciones del Responsable de la Seguridad son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Coordinar la realización de un análisis de riesgos, así como implantar los controles necesarios para reducir los riesgos.
- Reportar al Delegado de Protección de Datos sobre violaciones de seguridad de los datos personales.
- Difundir las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de la entidad.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Supervisar y velar por el cumplimiento de la normativa legal aplicable.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad acaecidos en la entidad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Se ha designado como Responsable de Seguridad a la persona recogida en el documento adjunto a la presente Política como **ANEXO II**.

Se adjunta en la presente Política como **ANEXO V** comunicado formal para la designación del Responsable de Seguridad, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

RESPONSABLES DEL SERVICIO

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado.

Las obligaciones del Responsable del Servicio son:

- Velar por el uso que se haga de determinados servicios y de la protección de estos.
- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Gestionar los tratamientos de datos personales, en cuanto al Reglamento 2016/ 679 General de Protección de Datos, por delegación del Responsable del Tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión del tratamiento de datos personales que se realizan en su área.

Se ha designado como Responsable/s de Servicio a la/s persona/s recogida/s en el documento adjunto a la presente Política como **ANEXO II.**

Se adjunta en la presente Política como **ANEXO III** comunicado formal para la designación de Responsables de Servicio, en el que se informa a los intervinientes acerca de sus principales funciones para el correcto cumplimiento de la Política de Seguridad de la entidad.

ADMINISTRACION DEL SISTEMA DE SEGURIDAD

La configuración y monitorización del sistema de seguridad (Firewall, Switches, EDR y SIEM) están externalizadas y delegadas en la empresa Cibersafety Soluciones S.L. con CIF B22456016 y domicilio social en la calle Vereda de Tabala, 58, Murcia.

6.4.- Difusión, actualización y revisión de la política de seguridad de la información

Será misión del Comité de Seguridad TIC 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 Órgano de Gobierno y esta será difundida para que la conozcan todas las partes afectadas.

La normativa de seguridad deberá estar a disposición de todos los miembros de la entidad.

Será el Responsable de Seguridad la persona encargada de la custodia y difusión de la versión aprobada de la documentación generada.

7.- DATOS DE CARÁCTER PERSONAL

La entidad trata datos de carácter personal. La política de Protección de Datos y las Medidas de Seguridad al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables de tratamiento correspondientes.

Todos los sistemas de información de la entidad 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.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las actividades de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará de este modo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

8.- GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política de Seguridad de la Información deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por la normativa, según lo previsto en el artículo 7 del ENS.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo autónomo, a través de un Plan de Adecuación al ENS.

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.

El análisis de riesgos también contemplará los requisitos establecidos por el artículo 32 del RGPD para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

9.- DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la entidad en diferentes materias:

1. Gestión de Accesos e Identidad

- **Normativa de Control de Acceso:** Define los criterios de concesión, revisión y revocación de permisos. Incluye la gestión de contraseñas, autenticación de doble factor (2FA) y el principio de "mínimo privilegio".
- **Política de Uso de Activos:** Reglas sobre el uso aceptable de equipos, correo electrónico e internet por parte de los empleados.

2. Desarrollo y Ciclo de Vida del Software (S-SDLC)

- **Normativa de Desarrollo Seguro:** Directrices para los equipos de desarrollo sobre el manejo de vulnerabilidades (OWASP), revisión de código y pruebas de seguridad.
- **Política de Gestión de Cambios:** Procedimientos para asegurar que las actualizaciones del sistema (incluyendo parches de seguridad) se realicen de forma controlada y documentada.
- **Normativa de Gestión de Vulnerabilidades:** Proceso para la detección, evaluación y mitigación de fallos técnicos en las aplicaciones.

3. Protección de Datos y Privacidad

- **Normativa de Criptografía y Cifrado:** Define qué algoritmos y longitudes de clave deben usarse para proteger los datos de pacientes y empleados, tanto en reposo como en tránsito.
- **Política de Retención y Destrucción de la Información:** (Vinculada al Plan de Capacidad) Establece los plazos legales para conservar datos y los métodos seguros para su eliminación definitiva.

- **Procedimiento de Gestión de Brechas de Seguridad:** Protocolo de actuación ante una fuga de datos, incluyendo la comunicación obligatoria a las autoridades de protección de datos.

4. Seguridad Operativa y en Comunicaciones

- **Normativa de Seguridad en Redes y Comunicaciones:** Reglas para la segmentación de redes, configuración de cortafuegos (firewalls) y seguridad en las integraciones HL7/FHIR.
- **Política de Copias de Seguridad (Backup):** Frecuencia, ubicación y pruebas de restauración de los datos críticos del sistema.
- **Normativa de Teletrabajo y Acceso Remoto:** Medidas de seguridad específicas (VPN, cifrado de disco) para el personal que trabaja fuera de las instalaciones de Tecnova.

5. Seguridad Física y del Personal

- **Normativa de Seguridad de Recursos Humanos:** Procedimientos de seguridad antes, durante y al finalizar la relación laboral (acuerdos de confidencialidad o NDAs).
- **Política de Limpieza de Escritorio y Pantalla:** Reglas para evitar la exposición accidental de información sensible en las oficinas.
- **Normativa de Seguridad Física y Ambiental:** Control de acceso a las instalaciones, salas de servidores y protección contra amenazas físicas (fuego, inundaciones).

6. Relación con Terceros y Continuidad

- **Normativa de Seguridad para Proveedores:** Requisitos de seguridad que deben cumplir los socios tecnológicos y proveedores de servicios en la nube de Tecnova.
- **Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP):** Estrategias para mantener la operatividad de los sistemas de salud en caso de fallos catastróficos.

7. Gestión de Incidentes

- **Normativa de Gestión de Incidentes de Seguridad:** Define cómo identificar, reportar y clasificar los incidentes, así como el equipo responsable de su resolución.

La normativa de seguridad estará a disposición de todos los miembros la entidad que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La política de seguridad se encuentra disponible en las instalaciones de la organización.

La normativa de seguridad estará a disposición de todos los miembros la entidad que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

10.- OBLIGACIONES DEL PERSONAL

Todos los miembros de la entidad 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 la entidad tendrán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Las sesiones de concienciación deberán quedar registradas mediante la cumplimentación del Anexo de la presente Política **REGISTRO DE ACCIONES FORMATIVAS VII.**

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

11.- TERCERAS PARTES

Cuando 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 la entidad 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. La entidad ha aprobado un procedimiento específico recogido en el documento **PROCEDIMIENTO DE REPORTE DE INCIDENTES DE SEGURIDAD.**

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.

12.- REFERENCIAS

La entidad debe incluir en este apartado todas las referencias documentales y legislativas que apoyan o completan esta Política de seguridad, o que se hayan tenido en cuenta a la hora de redactarla:

- Estándares internacionales (ISO/IEC 27001) y regulaciones del sector salud (GDPR, LOPDGDD, HIPAA).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico de Sector Público.
- Guía de Seguridad (CCN-STIC-815). Esquema Nacional de Seguridad Métricas e Indicadores.
- Guía de Seguridad de las TIC. CCN- STIC 817.
- El resto de normativa aplicable se encuentra en el apartado 3 “Legislación y Normativa aplicable”