APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 12 de abril del 2026 por el Responsable de seguridad.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política subida en apartado de documentación en Sofidya.

INTRODUCCIÓN

TICH CONSULTING depende de los sistemas TIC (Tecnologías 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, trazabilidad, autenticidad 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 anexo A según norma ISO 27002, 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.

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.

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.
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.

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 (CAU, Sistemas, otros departamientos).

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.

ALCANCE

Esta política se aplica a todos los sistemas TIC de TICH CONSULTING y a todos los miembros de la organización, sin excepciones a lo largo de todo el proceso de implementación de servicios de soporte, instalación, administración (remota e in-situ), desarrollo y mantenimiento del producto de software, HIS de GreenCube. Atendiendo a la declaración de aplicabilidad vigente.

MISIÓN

La misión de TICH Consulting es ofrecer a sus clientes soluciones eficientes para sus necesidades organizativas, poniendo a su disposición y al servicio de la innovación tecnológica y de gestión todo su conocimiento sobre el funcionamiento integral de los centros sanitarios.

OBJETIVOS Y COMPROMISOS

La Dirección, establece como objetivos de base, punto de partida y soporte de los objetivos y principios de la seguridad de la información los siguientes:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización.
- La protección de los derechos de propiedad intelectual.
- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.
- La formación y capacitación para la seguridad de la información.
- El registro de las incidencias de seguridad.
- La gestión de la continuidad del negocio.
- La gestión de los cambios que pudieran darse en la empresa relativos a la seguridad.

La Dirección, mediante la elaboración e implantación del presente Sistema de Gestión de Seguridad de la Información, adquiere los siguientes compromisos:

- Desarrollar software y servicios conformes con los requisitos legislativos, identificando para ello las legislaciones de aplicación a las líneas de negocio desarrolladas por la organización e incluidas en el alcance del Sistema de Gestión de la Seguridad de la Información.
- Establecimiento y cumplimiento de los requisitos contractuales con las partes interesadas.

- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento de planes de formación.
- Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento de acuerdos contractuales con organizaciones especializadas.
- Gestión de la continuidad del negocio, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- Establecimiento de las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
- Actuar en todo momento dentro de la más estricta ética profesional.

Esta Política proporciona el marco de referencia para la mejora continua del Sistema de Gestión de Seguridad de la Información, así como para establecer y revisar los objetivos del Sistema de Gestión de Seguridad de la Información.

MARCO NORMATIVO

A continuación, se indica el marco normativo relativo a la seguridad TI:

Reglamento (UE) 2016/679, General de Protección de Datos	Normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, protege los derechos y libertades fundamentales de las personas físicas
Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales	Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679, Garantizar los derechos digitales de la ciudadanía
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico	la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica
Real Decreto 1784/1996, de 19 de julio	Se aprueba el Reglamento del Registro Mercantil
Real Decreto Legislativo 1/1996, de 12 de abril	Se aprueba el texto refundido de la Ley de Propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016	Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

Real Decreto-ley 12/2018, de 7 de septiembre	Ley de seguridad de las redes y sistemas de información
Real Decreto-ley 28/2020, de 22 de septiembre	Referente al trabajo a distancia
Ley 2/2023, de 20 de febrero	Reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción

ORGANIZACIÓN DE LA SEGURIDAD

COMITÉS: FUNCIONES Y RESPONSABILIDADES

El comité de Seguridad TIC tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección general y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección general.
- 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 ENS 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad TIC estará formado por:

- **RESPONSABLE DEL SGSI:** Adjunto a dirección
- **RESPONSABLE DE SEGURIDAD:** Adjunto a dirección
- **RESPONSABLE DEL SISTEMA:** Subdirector de ingeniería de sistemas
- **RESPONSABLE DE SERVICIO:** Dirección de implantación, Proyectos y Sistemas
- **RESPONSABLE DE LA INFORMACIÓN:** Subdirector de ingeniería de sistemas

El secretario del Comité de Seguridad TIC: será la persona con puesto de adjunto a dirección: Bogdan Borovschi y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad TIC reportará a la Alta Dirección quien está representada por Director general : Luis Barcia Albacar.

ROLES: FUNCIONES Y RESPONSABILIDADES

Responsable de Seguridad: -

El responsable de Seguridad es el encargado de garantizar la seguridad de la información en una organización o entidad. Sus funciones y responsabilidades serán:

- Definir y mantener la política de seguridad de la información.
- Coordinar la implementación de las medidas de seguridad establecidas en el ENS y ISOs.
- Realizar evaluaciones de riesgos y planificar las acciones necesarias para mitigarlos.
- Supervisar la aplicación de controles de seguridad y asegurar su cumplimiento.
- Coordinar la respuesta a incidentes de seguridad.
- Mantenerse actualizado sobre las tendencias y novedades en materia de seguridad de la información.
- Representar a la organización ante las autoridades competentes en seguridad de la información.

Como responsable de la seguridad de la información se ha designado la persona con el puesto de Adjunto a dirección: Bogdan Borovschi

Responsable de Sistema:

El responsable de Sistema es el encargado de la gestión y operación de los sistemas de información en una organización. Sus funciones y responsabilidades serán:

- Tarea constante de analizar y detectar áreas de mejora y desarrollar nuevas soluciones que aumenten la eficiencia.
- Definir, planificar, realizar y controlar actividades y los tiempos para lograr objetivos específicos.
- Implementación de tecnologías avanzadas
- Toma de decisiones relacionadas con los servicios y procesos de entrega de cada proyecto
- Administrar y mantener los sistemas de información de acuerdo con las normas y requisitos del ENS.
- Coordinar la implementación de medidas de seguridad técnicas en los sistemas.

- Supervisar el mantenimiento, actualización y parcheo de los sistemas.
- Realizar copias de seguridad y asegurar la recuperación de datos en caso de incidentes.
- Monitorear y analizar el rendimiento de los sistemas.
- Implementar y mantener las medidas de continuidad del negocio.
- Colaborar con el responsable de Seguridad en la gestión de riesgos y en la respuesta a incidentes.

Como responsable de sistema se ha designado la persona con el puesto de Subdirector de ingeniería de sistemas: José Luis Gálvez

Responsable de Servicio: -

El responsable de Servicio es el encargado de la gestión de los servicios de TI en una organización. Sus funciones y responsabilidades serán:

- Definir y gestionar el catálogo de servicios de TI de acuerdo con el ENS.
- Coordinar la implementación y provisión de los servicios de TI.
- Garantizar la disponibilidad, integridad y confidencialidad de los servicios.
- Supervisar la resolución de incidencias y problemas relacionados con los servicios.
- Realizar evaluaciones periódicas de los servicios y proponer mejoras.
- Colaborar con el responsable de Seguridad en la gestión de riesgos y en la implementación de controles de seguridad en los servicios.

Como responsable del servicio se ha designado a la persona con puesto DIRECCIÓN DE IMPLANTACIÓN, PROYECTOS Y SISTEMAS: Miguel Ortiz García.

Responsable de la Información: -.

El responsable de la Información es el encargado de la gestión de la información en una organización. Sus funciones y responsabilidades serán:

- Identificar y clasificar la información en función de su importancia y nivel de protección requerido.
- Establecer y mantener las políticas y procedimientos para la gestión de la información.
- Coordinar la implementación de controles de acceso y protección de la información.
- Garantizar el cumplimiento de las normativas y requisitos legales relacionados con la información.

- Supervisar el manejo adecuado de la información, incluyendo la transferencia y el almacenamiento seguro.
- Colaborar con el responsable de Seguridad en la gestión de riesgos y en la respuesta a incidentes relacionados con la información.

Como responsable de la información se ha designado la persona con el puesto de Subdirector de ingeniería de sistemas: José Luis Gálvez

PROCEDIMIENTOS DE DESIGNACIÓN

El responsable de SGSI será nombrado por la **Dirección general** a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo con la Ley 11/2007 designará al responsable del Servicio, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

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 la Alta Dirección y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

TICH CONSULTING trata datos de carácter personal por lo que ha establecido un procedimiento de tratamiento y gestión de estos, gestionado directamente por DPO externo.

Este documento colgado en nuestra página web www.tichconsulting.comdescribe:

- El análisis de riesgos de privacidad.
- Las medidas de seguridad de protección de datos.
- Los procedimientos asociados a derechos de los interesados.
- Los contratos con terceros para el tratamiento de datos personales.

Asimismo, el documento incluye un registro de actividades de tratamiento de datos personales, desglosando:

- El tipo de tratamiento afectado.
- La base jurídica y los fines del tratamiento.
- Las categorías de datos personales.

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

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.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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

- Política de uso aceptable de activos.
- Política de gestión de contraseñas.
- Política de control de accesos.
- Política de controles criptográficos.
- Política de desarrollo.
- Política de uso de servicios en la nube.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en Sofidya, en apartado de documentos.

OBLIGACIONES DEL PERSONAL

Todos los miembros de TICH CONSULTING tienen la obligación de conocer y cumplir estas Políticas 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 TICH 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 TICH CONSULTING, 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

TERCERAS PARTES

Cuando TICH 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 TICH 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.

MECANISMOS DE COORDINACIÓN Y RESOLUCION DE CONFLICTOS DE SEGURIDAD DE LA INFORMACIÓN.

TICH CONSULTING ha establecido que para la coordinación y resolución de conflictos que se presenten respecto a la seguridad de la información serán debatidos, investigados y tratados por el comité de seguridad siguiendo los procedimientos establecidos.

Se dejará constancia del tema tratado y las decisiones tomadas en un acta.

Alta Dirección

Alicante, 12 de Abril de 2026

Luis Barcia Albacar

Bogdan Borovschi