Contenido

Este documento impreso estará vigente siempre que la edición que en él figura coincida con la del archivo informático correspondiente ubicado en el servidor informático de la Empresa.

1. Aprobación y entrada en vigor

Texto aprobado el día 25 de febrero de 2026 por el Director General. Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación (o publicación para las entidades que sea obligatoria su publicación oficial) y hasta que sea reemplazada por una nueva Política.

Este texto deroga al anterior, que fue aprobado el día 01 de octubre de 2025 por Dirección General.

2. Introducción

La Dirección de la Sociedad Concesionaria Gran Hospital Can Misses, en adelante SCGHCM, en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la organización, aprueba la siguiente Política de Seguridad de la Información del Esquema Nacional de Seguridad (en adelante, ENS). El objetivo de esta Política es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información de los sistemas que se encuentran sujetos al ENS.

3. Objeto

Establecer las directrices y principios que regirán el modo en que SCGHCM gestionará y protegerá su información y sus servicios, cumpliendo con los objetivos y directrices de la Política de Seguridad de la Información corporativa, a través de la implantación, mantenimiento y mejora de un SGSI y aplicando los requisitos y medidas de seguridad dentro del marco regulatorio del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que exige el establecimiento de los principios básicos y requisitos mínimos en la utilización de medios electrónicos que permita la adecuada protección de la información y los servicios.

4. Alcance

Tomando en cuenta el contexto en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones en el cumplimiento, esta Política se circunscribe a los servicios y sistemas incluidos en el alcance del ENS que dan cobertura al cumplimiento de los requisitos y medidas de seguridad establecidas en el Esquema Nacional de Seguridad en lo relativo a:

- Servicios internos de gestión propios de la SCGHCM.
- Servicio de gestión del archivo de historias y documentación clínica.

- Servicio de restauración.
- Servicio de logística.
- Servicio de lavandería y lencería.
- Servicio de limpieza e higienización.
- Servicio de seguridad y vigilancia.
- Servicio de mantenimiento de instalaciones.
- Servicio de desinsectación y desratización.
- Servicio de jardinería y cuidados exteriores.
- Servicio de gestión telefónica y citación de pacientes.
- Servicio de aparcamiento.
- Servicio de televisión, telefonía e internet.
- Servicio de máquinas vending.
- Servicio de cafetería-bar y comedor.
- Servicio de guardería y ludoteca.
- Servicio de locales comerciales.

El ámbito de aplicación es el centro situado en Calle Corona, s/n 07800 Eivissa, Illes Balears.

5. Misión

GHCM tiene como misión para sí misma y para todos los centros que gestione:

- Promover un ambiente de trabajo seguro y saludable para los empleados de GHCM y Operadora Can Misses, minimizando los riesgos que no se pueden evitar.
- Utilizar la formación y la información como principales herramientas para la lucha contra los accidentes laborales.
- Asegurar un buen clima laboral dentro de la empresa que motive y proporcione satisfacción a los empleados de GHCM y Operadora Can Misses.
- Aplicar una política integral de personal dirigida al conjunto de colaboradores que desarrollan los servicios no clínicos del hospital, con el objetivo de crear un entorno dinámico basado en la seguridad, la eficiencia, la calidad, el respeto y el crecimiento profesional y humano.
- Emplear un sistema de gestión por procesos que, incorporando las últimas herramientas tecnológicas y organizativas, garantice en todo momento los máximos niveles de eficiencia y calidad.
- Disponer de un sistema integral de Información que posibilite la integración con los sistemas del hospital, ofreciendo un entorno de gestión práctico y sencillo.
- Implantar un sistema de cooperación y coordinación permanente con su entorno.

6. Principios rectores y objetivos

Mediante esta Política, SCGHCM asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

a) Garantizar el cumplimiento con los objetivos y principios generales detallados en la Política de Seguridad de la Información aprobada y promovida por la Dirección de la empresa.
b) Asegurar el establecimiento y cumplimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de la empresa.
c) Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la sociedad.
d) Asegurar que los recursos necesarios para el ENS estén disponibles.
e) Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
f) Asegurar que el ENS consigue los resultados previstos.
g) Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
h) Promover la mejora continua.
i) Asegurar la vigilancia continua.
j) Realización de reevaluaciones periódicas.
k) Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

a) Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
b) Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
c) Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
d) Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
e) La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Asimismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta lo que se va a hacer, los recursos necesarios, el responsable y el plazo de consecución.

7. Marco legal y regulatorio

a) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
b) 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.
c) Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
d) Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
e) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
g) Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
h) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
i) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
j) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
k) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Adicionalmente, SCGHCM cuenta con un registro pormenorizado de toda la legislación que es aplicable a los servicios del Sistema de Gestión y del ENS.

8. Organización de la seguridad

La Dirección de SCGHCM tiene como responsabilidad fundamental la de liderar y comprometerse con respecto al ENS.

8.1. Mecanismos de coordinación y Comités

SCGHCM cuenta con un Comité de Seguridad de la Información que dispone de las siguientes funciones:

- Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el SGSI y el cumplimiento del ENS.
- Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente y resto de partes interesadas en todos los niveles de la organización.
- Aprobación del análisis de riesgos
- Aprobación, en su caso, del Plan de Tratamiento de Riesgos (PTR)
- Sus miembros, como tales, deben aceptar sus puestos y funciones

La composición del Comité de Seguridad de la Información (CSI) se establece en el apartado 5.4 del Manual del Sistema de Gestión de Seguridad de la Información.

8.2. Funciones y responsabilidades de seguridad

a) **Responsable de la Información:**
- Determina los requisitos de la información tratada
- Tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. El responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información). El ENS asigna al responsable de la información la potestad de establecer los requisitos y los niveles de seguridad necesarios para la información en materia de seguridad.
- El responsable de la información aprueba el documento de valoración del sistema
- El responsable de la información aprueba, como parte del análisis de riesgos, los riesgos residuales
- Debe aceptar su perfil de puesto y funciones

b) **Responsable del Servicio:**
- Determina los requisitos de los servicios prestados, incluyendo las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas
- El ENS asigna al responsable del servicio la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar

los niveles de seguridad de los servicios, pudiendo ser una persona física concreta o un órgano colegiado.

- El responsable del servicio también aprueba el documento de valoración del sistema
- El responsable del servicio aprueba, como parte del análisis de riesgos, los riesgos residuales
- Debe aceptar su perfil de puesto y funciones

c) **Responsable del sistema:** que tendrá las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Propone la valoración del sistema
- Debe adoptar las medidas correctoras derivadas de las auditorías (PAC)
- Debe aceptar su perfil de puesto y funciones

d) **Responsable de Seguridad (desempeñado por el RSGSI):** Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Además, será responsable de las siguientes funciones incluidas y descritas de manera más amplia en el Manual del Sistema de Gestión:

- Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones
- Velar por el cumplimiento de las políticas de seguridad
- Gestionar y desarrollar los análisis de riesgos de seguridad de la información
- Desarrollar, impulsar, coordinar e implementar la Política de Seguridad de la Información
- Elaborar e implementar los procedimientos e instrucciones técnicas en materia de seguridad de la información.
- Recomendar los controles de seguridad aplicables a los sistemas de información para reducir el riesgo.
- Recomendar las actividades de diseño, evaluación, selección e implementación de soluciones de Seguridad de la Información.
- Promover la formación y concienciación en materia de seguridad de los sistemas de información y las redes de comunicaciones que los soportan, tanto en aspectos lógicos, físicos y organizativos.
- Investigar los incidentes de seguridad de la información.
- Notificar al CSI incidentes de seguridad que tengan impacto en la prestación de los servicios

- Dirigir la actividad de Seguridad de la Información, que dispondrá de los medios técnicos y humanos necesarios para asumir todas las funciones que tiene asignadas, tanto organizativas como técnicas. Cualesquiera otras funciones que se recojan en la legislación vigente en la materia.
- Propone la valoración del sistema
- Determinación de la categoría del sistema
- Aprobación de la Declaración de Aplicabilidad (SoA)
- Aprobación del Análisis de Riesgos
- Debe aceptar su perfil de puesto y funciones

e) **POC (Punto o Persona de Contacto)** para la seguridad de la información tratada y el servicio prestado, cuenta con el apoyo de los órganos de dirección, y canaliza y supervisa, 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 POC de seguridad es el propio Responsable de Seguridad de la organización. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.
   - Debe aceptar su perfil de puesto y funciones.

f) **Responsable de Seguridad protección datos personales**: Velar por el cumplimiento de los requisitos en materia de protección de datos de carácter personal.

g) **Administrador del sistema:** Cumplimiento de los procedimientos técnicos de seguridad de la información.

h) **Administradores funcionales de aplicaciones:** Altas, bajas y gestión de privilegios en las aplicaciones.

8.3. Designación de funciones

La Dirección asegura, con la colaboración del RSGSI, que el personal dispone de la necesaria formación teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Las funciones y responsabilidades inherentes a cada puesto de trabajo dentro del SGSI, así como los requisitos de formación y experiencia necesarios, están recogidas en los perfiles de puesto de trabajo, debiendo ser aprobadas las modificaciones por la dirección en el CSI.

El registro que designa a las personas que realizan las funciones descritas es el "FPR-BA-52-01 Listado de funciones vs responsables Ed 02".

Los nombramientos podrán ser revisados cada año, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento. SCGHCM debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de

ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

8.4. Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno de la Dirección que podrá delegar sus funciones en el Comité de Seguridad de la Información.

Tanto los nombramientos como la posible resolución de conflictos correrán a cargo de la Dirección.

9. Formación y concienciación

Dentro de los planes de formación se incluirán acciones de concienciación orientadas al personal de forma que se realice una concienciación relativa, entre otros, a los siguientes aspectos:

- Política de seguridad de la información.
- Seguridad de la información.
- Riesgos, vulnerabilidades y amenazas de los sistemas de información.
- Necesidad del cumplimiento de la legislación vigente

10. Gestión de riesgos

Las actividades objeto de esta política de seguridad incluidas en el ámbito del ENS tiene su correspondiente 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
- cuando se realice cualquier cambio significativo del sistema o del SGSI

Para la armonización del análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones a realizar.

SCGHCM utiliza la herramienta PILAR siguiendo la metodología Magerit v.3 para la realización del análisis de riesgos. Los resultados del mismo se pueden consultar sobre la propia herramienta y/o sobre el informe "SCGHCM Gestión del Riesgo-01 Análisis y Valoración".

11. Datos de carácter personal

El tratamiento de datos de carácter personal se basará en la "Política de Protección de Datos", en la que se fijan las directrices que se deben seguir para garantizar la privacidad de los datos de los clientes, proveedores, empleados y, en general, de todos los colectivos de datos implicados, identificando la base de legitimación más adecuada para los tratamientos de datos personales llevados a cabo de acuerdo con la legislación vigente.

12. Obligaciones del personal

Todos los miembros de SCGHCM tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de SCGHCM, a través del Comité de Seguridad y del área de personal, de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de SCGHCM atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de SCGHCM, 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.

13. Terceras partes

Cuando SCGHCM preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando SCGHCM 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, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

Este documento impreso estará vigente siempre que la edición que en él figura coincida con la del archivo informático correspondiente ubicado en el servidor informático de la Empresa.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las guías que las desarrollan.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que SCGHCM pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales, por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

14. Gestión de incidentes de seguridad

SCGHCM dispone de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

15. Documentación

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema Integrado de Gestión que se recogen en el documento "SCGHCM-Manual del Sistema de Gestión".

Toda la información documentada relativa al Sistema Integrado de Gestión se aloja en los Sistemas de Información de SCGHCM.

16. Aprobación y entrada en vigor

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.