Contenido

- Anexo APR-BA-44-01 Política de privacidad corporativa
- Anexo APR-BA-44-02 Política de Regalos
- Anexo SCGHCM - ENS - Política de seguridad

1. Introducción

El presente Código Ético de Conducta se desarrolla con el objetivo de establecer y preservar los valores éticos que deben guiar el comportamiento de todos los empleados, colaboradores y socios de negocio, con la finalidad de asegurar la eficacia y profesionalidad de sus actuaciones en el ejercicio de su actividad.

2. Objeto

Este Código Ético de Conducta (en adelante, el Código) tiene por finalidad establecer los principios éticos que deben regir la actuación de los empleados, directivos y consejeros de **GHCM/OPERADORA**, así como sus socios de negocio, y determinar las principales normas de actuación que deben cumplir las personas que trabajan y participan en la actividad de la empresa., estableciendo, igualmente, una serie de compromisos y políticas de actuación.

Forma parte de la cultura de la empresa asentar las actuaciones de **GHCM/OPERADORA** sobre los valores de **integridad, excelencia, confianza y sostenibilidad**, alineando nuestra conducta con los valores que redunden mayor beneficio para la sociedad y nuestra organización.

Estos principios y normas tienen carácter general, no obstante, en aquellas áreas en que se considere adecuado disponer de una regulación específica, se desarrollarán procedimientos, protocolos, normativas internas y manuales que incluyan entre otros, los siguientes documentos:

- ✓ Normativa interna y procedimientos.
- ✓ Guía o Plan de Prevención de Riesgos Laborales.
- ✓ Manual de Gestión de Calidad y Medio Ambiente.
- ✓ Política y Manual de *Compliance* penal.
- ✓ Política de privacidad corporativa
- ✓ Acuerdo de confidencialidad y secreto profesional.

3. Personas obligadas

Todos los empleados y directivos de **GHCM/OPERADORA**, así como sus socios de negocio, tienen la obligación de conocer y cumplir el Código, con independencia de la modalidad contractual que regule su relación jurídica o del puesto en el que desempeñen su trabajo. Las personas obligadas tienen además la obligación de conocer y cumplir la normativa y, en particular, los manuales, procedimientos, instrucciones técnicas o guías que se refieren a su actividad especifica.

Los incumplimientos del código y de la normativa darán lugar a la imposición de sanciones disciplinarias, de acuerdo con lo que determina el Derecho Laboral y con lo establecido en el código disciplinario de la organización, sin perjuicio de las sanciones administrativas o penales que en su caso puedan derivarse de tal incumplimiento. El cumplimiento del código y la normativa forma parte de las obligaciones inherentes a la relación laboral.

Las personas obligadas que tengan conocimiento de cualquier incumplimiento del código o de la normativa deberán comunicarlo al Órgano de Cumplimiento Penal (el OCP).

Aunque **GHCM/OPERADORA** no puede hacerse responsable de la actuación de terceros con los que mantiene relaciones contractuales, su propósito es que todas las personas y empresas contratadas cumplan con sus estándares y principios éticos, especialmente los proveedores, agentes, consultores y empresas subcontratadas. Por ello, el OCP velará por que se informe a dichas terceras empresas del contenido de este código y de que los contratos que se suscriban con ellas recojan las exigencias del código y, en su caso, de la normativa que sea de aplicación.

4. Cumplimiento y supervisión del Código Ético de Conducta

El órgano encargado del cumplimiento y supervisión del Código es el Órgano de Cumplimiento Penal (en adelante, "OCP"). Dicho órgano está formado por cuatro miembros, tal como se establece en el procedimiento **[PR-BA-40 Órgano de Cumplimiento Penal]**.

En lo que respecta a este Código, la principales funciones y obligaciones de este órgano son:

- Supervisar el cumplimiento del código y la normativa.
- Interpretar las normas emanadas del Código y supervisar la aplicación de estas.
- Promover la difusión, el conocimiento y el cumplimiento del Código.
- Establecer las vías de comunicación oportunas para que cualquier empleado pueda recabar o facilitar información sobre su cumplimiento, garantizando en todo momento la confidencialidad de las denuncias que se tramiten.
- Garantizar la veracidad y ecuanimidad de cualquier procedimiento iniciado, así como los derechos de las personas presuntamente implicadas en un posible incumplimiento.
- Definir los casos en los que el ámbito de aplicación del Código debe hacerse extensivo a terceros que vayan a mantener relaciones comerciales o empresariales con GHCM/OPERADORA.
- Llevar a cabo reuniones anuales para realizar el seguimiento del cumplimiento del Código y levantar acta de dichas reuniones.

Todos los departamentos de **GHCM/OPERADORA** están obligados a colaborar con el OCP en el desarrollo de su función de cumplimiento en cualesquiera peticiones que les formulen.

El adecuado conocimiento del Código y de la normativa requiere su conocimiento por parte de todas las personas obligadas. Para conseguir este fin, el OCP se encargará de la difusión y conocimiento del Código, a través de los canales de comunicación a disposición de los empleados, como son las publicaciones en el tablón de anuncios, y en la web corporativa https://ghcanmisses.es/.

Desde el departamento de RR.HH., junto con el OCP, se planificarán los cursos de formación necesarios para que todos los empleados de **GHCM/OPERADORA** conozcan el código y la normativa que afecten a su actividad. La persona responsable de RR.HH., como responsable de formación, mantendrá un registro de todos los cursos de formación realizados por los empleados y resto de personas obligadas, debiendo conservar una acreditación documental de la efectiva realización de la formación.

El OCP colaborará a fin de que los materiales de formación que elabore la responsable de RR.HH se ajusten al contenido del Código y la normativa.

Al inicio de la relación laboral con **GHCM/OPERADORA**, se entregarán a los trabajadores tanto el Código como la normativa.

El Código se revisará cuando sea necesaria su actualización por cambios legislativos o para adaptarlo a la realidad de la Sociedad Concesionaria, tras lo cual será aprobado por el OCP.

5. Canal Interno de comunicaciones. Canal Ético

La **GHCM/OPERADORA** dispone de un Canal Interno de comunicaciones, de conformidad con "Ley 2/2023 de 20 de febrero, de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción" a través del cual cualquier empleado que tenga conocimiento de un incumplimiento del presente Código, de la normativa en vigor, de políticas internas, así como de cualquier acto ilícito cometido en la empresa, podrá comunicarlo con plenas garantías y sin temor a sufrir ninguna represalia. Es la herramienta de comunicación principal de la organización para conocer los incumplimientos y hacer respetar nuestros valores y compromisos.

Este Canal de Información está abierto a todos los grupos de interesados relacionados con SCGHCM/OPERADORA, enumerados en el art. 3 de la Ley de Protección del informante, tales como: empleados, extrabajadores, becarios y voluntarios; autónomos; accionistas y miembros del órgano de administración, contratistas y subcontratistas; proveedores; y, en general, terceros con relación directa con la empresa.

El Canal de Información permite la comunicación por escrito, mediante: formulario on-line https://comunicaciones.targatis.com/es; correo electrónico canaleticoghcm@targatis.com; correspondencia postal a: Waterwale Europe, S.L.P- A/A Concesionaria Can Misses , C/ María Zambrano, 31, Torre Oeste, P13, 50018- Zaragoza (España);y mediante solicitud de reunión presencial a través de cualquiera de los medios anteriormente citados.

Se mantendrá una estricta confidencialidad sobre la identidad de la persona que realice cualquier comunicación o denuncia a través del Canal Ético, o en su caso, anonimato, si así lo considera.

En ningún caso se tolerará ninguna forma de represalia o medida negativa de cualquier clase contra un empleado de la **GHCM/OPERADORA** por el hecho de haber comunicado o denunciado un presunto incumplimiento del Código o de la normativa.

El Canal Ético no ampara las denuncias falsas o manifiestamente infundadas. Cuando exista evidencia de que la denuncia falsa se ha realizado de mala fe, el departamento de RR.HH. adoptará las medidas

disciplinarias que sean procedentes. En la tramitación de las denuncias se respetará el derecho de defensa de la persona denunciada y la normativa de protección de datos.

Toda la información relativa al Sistema Interno de Comunicación se encuentra disponible en la web corporativa de la empresa, en el enlace: https://ghcanmisses.es/canal-etico-de-comunicacion/

A. PRINCIPIOS GENERALES

6. Principios generales y valores que promovemos.

6.1. Integridad

Todas las personas obligadas desarrollarán su actividad con integridad y cumpliendo con principios éticos. En ningún caso se admitirá como razón o excusa que un comportamiento no ético beneficia a la **GHCM/OPERADORA**. La empresa rechaza cualquier beneficio que proceda de una actuación ilegal.

6.2. Lealtad

Las personas obligadas deben actuar con lealtad hacia la empresa, evitando entrar en situaciones que supongan un conflicto entre los intereses de **GHCM/OPERADORA** y sus intereses particulares. En caso de que un conflicto de interés sea inevitable, informarán del mismo a su superior o también al órgano encargado de cumplimiento y se abstendrán de intervenir en las decisiones afectadas por dicho conflicto.

6.3. Confidencialidad

Las personas obligadas mantendrán una estricta confidencialidad sobre toda la información no pública que conozcan en el ejercicio de su trabajo. Esta obligación de confidencialidad deberán respetarla aun después de cesar su relación profesional con la Sociedad Concesionaria. El deber de confidencialidad se extiende a cualquier información no pública de terceros de la que se disponga en virtud de las relaciones comerciales o empresariales que la Sociedad Concesionaria mantenga con ellos. Para ello, los empleados de **GHCM/OPERADORA** suscriben un acuerdo de confidencialidad y secreto profesional, al iniciar su actividad en la organización en el momento de firmar su contrato de trabajo.

6.4. Cumplimiento de las normas

Las personas obligadas deberán desempeñar sus funciones cumpliendo con la legislación aplicable vigente (leyes, reglamentos, circulares, etc.) y evitando cualquier práctica que no sea éticamente aceptable bajo estrictos criterios de honestidad e integridad moral.

Igualmente, cumplirán con la normativa interna de la **GHCM/OPERADORA** y con cualquier otro reglamento interno de conducta aplicable a su actividad cuyas normas establezcan obligaciones más rigurosas que las recogidas en este Código.

6.5. Oposición a los actos de corrupción

En las relaciones con las Administraciones Públicas y con terceras empresas, ya sean clientes o proveedores, no se realizará ninguna actuación que pueda interpretarse como una forma de obtener indebidamente una decisión favorable a **GHCM/OPERADORA** o un trato de favor para ésta. La Sociedad Concesionaria rechaza de forma rotunda toda forma de corrupción, tanto en el ámbito público como en el privado, comprometiéndose con la lucha contra el soborno.

6.6. Igualdad de oportunidades

GHCM/OPERADORA promueve el desarrollo profesional y personal de todos sus empleados asegurando la igualdad de oportunidades. Las políticas de contratación y promoción de personal, en ningún caso, contendrán prácticas discriminatorias. Todo tratamiento discriminatorio a empleados, proveedores o clientes que violen los valores éticos, será penalizado con las medidas disciplinaria apropiadas. Por ese motivo, el **Plan de Igualdad** elaborado por la empresa reconoce este principio general, entre otros.

6.7. Prohibición del acoso laboral

Cualquier forma de acoso laboral está absolutamente prohibida en **GHCM/OPERADORA** y, en caso de producirse, tendrá una respuesta enérgica por parte de la empresa. Tal y como se recoge en el **Protocolo de actuación y prevención del acoso psicológico, acoso sexual o por razón de sexo**, que se entrega a todos los trabajadores de **GHCM/OPERADORA** en el momento de su incorporación.

Todos los empleados, proveedores o clientes deben ser tratados de forma justa y con respeto por parte de superiores, subordinados y compañeros. No se tolerará ningún tipo de conducta abusiva, hostil u ofensiva, tanto verbal como física.

6.8. Veracidad de la información

Todos los empleados deben suministrar una información veraz, completa, comprensible y puntual acerca de la marcha de las actividades relacionadas con su trabajo. En ningún caso, proporcionarán a sabiendas información incorrecta, inexacta o imprecisa que pueda inducir a error a quien la recibe.

Las personas obligadas deberán velar por el prestigio y la buena imagen de la organización.

GHCM/OPERADORA se compromete a mantener una política de formación para el aprendizaje y el desarrollo personal y profesional de sus empleados con el fin de alcanzar el mayor rendimiento, calidad y satisfacción en la realización de sus funciones.

GHCM/OPERADORA pone a disposición de sus empleados los recursos necesarios para el desempeño de su actividad profesional y se compromete a facilitar los medios adecuados para la protección y salvaguarda de estos. Todos los empleados deben utilizar los recursos de la empresa de forma responsable, eficiente y apropiada al entorno de su actividad profesional, tal como se establece en el protocolo de seguridad de la información [**SCGHCM - ENS - Política de seguridad**]. Asimismo, deben protegerlos y preservarlos de cualquier pérdida, daño, robo o uso ilegal o deshonesto.

B. PRINCIPIOS ESPECÍFICOS POR ÁREAS

7. Prevención de Riesgos Laborales

GHCM/OPERADORA tiene un firme y permanente compromiso con la seguridad y la salud en el trabajo, así como con el cumplimiento escrupuloso de toda la normativa que resulta de aplicación en la materia, de modo que este compromiso constituye un valor esencial en el desarrollo de sus actividades.

GHCM/OPERADORA proveerá a todos sus empleados de los medios y recursos necesarios para que puedan llevar a cabo sus cometidos laborales en condiciones de seguridad, y sus empleados deberán realizar un uso responsable de los mismos.

Todos los empleados de la organización asumen la responsabilidad de dar un cumplimiento riguroso a las normas de seguridad y salud laboral, en el desempeño de sus actividades, velando por su propia seguridad y por la de quienes les rodean. De igual modo, los empleados divulgarán entre sus compañeros y subordinados su conocimiento en la materia y promoverán el cumplimiento de las mejores prácticas de protección y prevención de riesgos.

Todos los empleados son responsables de cumplir rigurosamente las normas de salud y seguridad. Asimismo, cuando desarrollen actividades de riesgo, deberán hacer uso responsable del equipamiento que tengan asignado y divulgarán entre sus compañeros y subordinados los conocimientos en este ámbito y promoverán el cumplimiento de las prácticas de prevención de riesgos laborales.

8. Protección del Medio Ambiente

GHCM/OPERADORA tiene una especial preocupación por la preservación y el respeto al entorno medioambiental, para lo cual aplica una estrategia medioambiental que permite prevenir y, eventualmente, minimizar los efectos negativos que sus actividades pudieran ocasionar.

GHCM/OPERADORA desarrolla su actividad asumiendo el firme compromiso de preservar y respetar el medio ambiente, sobre la base de los siguientes principios:

- Contribuir a la conservación de los recursos naturales, que se consumirán, en todo caso, con criterios de racionalidad, eficacia y ahorro.
- Reducir la generación de residuos, gestionarlos adecuadamente y fomentar su reutilización.
- Formar e informar al personal en materia medioambiental.

De lo que se desprende que **GHCM/OPERADORA** se compromete al estricto cumplimiento de la legislación medioambiental que le sea de aplicación.

9. Política Anticorrupción

GHCM/OPERADORA prohíbe por completo cualquier tipo de soborno a autoridades, funcionarios públicos o directivos o empleado pertenecientes a empresas u organismos públicos, así como, a ningún tercero con el que la empresa mantenga cualquier tipo de relación, ya sea un ente público o un particular. Por ello, a través de su Sistema de Gestión de *Compliance* Penal (SGCP), ha establecido acciones para mitigar el riesgo de los delitos penales, en particular: los delitos de corrupción en los negocios, cohecho y tráfico de influencias.

En consecuencia, está terminantemente prohibida la realización, promesa u ofrecimiento de ningún tipo de pago a autoridades, funcionarios públicos o directivos o empleados pertenecientes a empresas u organismos públicos o privados, ya se haga de manera directa, ya se haga de forma indirecta a través de agentes, intermediarios, asesores o cualesquiera personas interpuestas.

Tampoco está permitida la obtención de ventajas indebidas fruto del aprovechamiento de relaciones personales con autoridades o funcionarios públicos o con cualquier otro sujeto pasivo.

La organización exige que todas las decisiones adoptadas por aquellos empleados suyos que mantengan algún tipo de relación con las administraciones públicas se hagan con estricto respeto a la ley aplicable y a la normativa.

9.1. Intermediarios, agentes y asesores

La contratación de asesores o intermediarios en operaciones o transacciones en las que de algún modo intervenga una administración, organismos o empresa pública, se ajustará a las más estrictas exigencias derivadas de la diligencia debida.

Las personas obligadas que participen en procesos de selección de proveedores, subcontratistas y colaboradores externos, tienen la obligación de actuar con imparcialidad, transparencia y objetividad, aplicando criterios de calidad y coste para obtener la oferta más conveniente. Éstos deben abstenerse de participar en aquellos procesos en los que se produzca la colisión de sus intereses personales con los de la **GHCM/OPERADORA**.

Se informará a los asesores e intermediarios de todas aquellas prohibiciones que la organización ha articulado en materia de corrupción, y éstos manifestarán su conocimiento de tales prohibiciones y compromiso de riguroso cumplimiento, acusándose recibo de la comunicación y puesta a disposición de la información concreta.

9.2. Regalos, obsequios, atenciones y favores

La Sociedad Concesionaria prohíbe a sus empleados dar o aceptar regalos, obsequios, atenciones o favores en el desarrollo de sus actividades, siempre que el ofrecimiento pueda condicionar ilícitamente la conducta del que recibe el objeto de valor.

De manera excepcional, se admitirá la entrega o recepción de regalos y obsequios, siempre que no estén prohibidos por la ley, se correspondan con prácticas comerciales o signos de cortesía normales y usuales,

generalmente aceptados, se entreguen o reciban sin espera de reciprocidad y tengan en todo caso un valor económico simbólico o irrelevante, siendo ocasionales y no excesivos, conforme a los estándares locales o de la actividad.

Con el objeto de definir un marco orientativo del valor económico de referencia para empleados, responsables de área y jefes de servicio se establece un límite máximo de 100 euros. En el caso de directivos, el valor del obsequio o atención no sería recomendable que superase un importe de 100 euros. En consecuencia, en caso de duda, se optará por consultar al superior jerárquico o no dar o aceptar el regalo, obsequio o atención ofrecido.

GHCM/OPERADORA ha desarrollado la política de regalos en mayor detalle, en el documento anexo, APR-BA-44-02, donde se define un marco de actuación en términos honestidad, responsabilidad, integridad, imparcialidad y transparencia que debe aplicarse en todas las transacciones de negocio, garantizando prácticas comerciales éticas que eviten conflictos de interés.

La Política de Regalos, se aplica a todos los empleados, directivos, contratistas, proveedores, clientes, así como a cualquier otra parte interesada o socio de negocio que interactúe con SCGHCM/ OPERADORA. Todos ellos, tienen la obligación de conocer y cumplirla, con independencia de la modalidad contractual que regule su relación jurídica o del puesto en el que desempeñen su trabajo.

10. Política de Seguridad de la Información y Protección de datos

GHCM/OPERADORA, asume la seguridad de la información asociada a sus servicios como uno de los factores clave en la realización de sus actividades con objeto de garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos y los sistemas de información contra accesos y uso indebidos y modificaciones no autorizadas.

Los pilares son:

- La orientación de nuestros esfuerzos va dirigida a la prevención de errores, en lugar de a su control y corrección.
- La participación de todos es clave para conseguir los objetivos establecidos por GHCM lo que redundará en beneficio para nuestros clientes.
- La formación continua y la concienciación del personal es elemento básico.
- Asegurar que la empresa cumple con los requisitos de los clientes además de con los requisitos legales y reglamentarios aplicables, haciendo especial foco en aquellos establecidos por la legislación en materia de seguridad de la información.
- Establecer acciones sistemáticas de control, monitorización y prevención de incidentes
- Garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.
- Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos.

GHCM/OPERADORA entiende que los procesos asociados a la seguridad de la información no pueden imponerse desde fuera, sino que deben nacer desde el interior de su equipo humano. Por ello, anima a todo el personal de GHCM a hacer de la seguridad de la información su forma de trabajo

GHCM/OPERADORA pone a disposición de sus empleados los recursos informáticos que considera convenientes para el desarrollo de su trabajo, lo que implica respetar los derechos de otros usuarios, la integridad de las instalaciones, y los acuerdos y contratos con terceros cuando sea aplicable. Cada persona que preste sus servicios en la empresa y tenga debidamente autorizado el acceso al sistema informático, tendrá asignado un equipo informático concreto o estación de trabajo para el desarrollo de su actividad, y tendrá acceso únicamente a sus aplicaciones y ficheros de datos personales necesarios para el desempeño de sus funciones.

Para la protección de dichos recursos, **GHCM/OPERADORA** ha establecido las medidas de seguridad oportunas y el personal con acceso a ellos debe ser responsable de su aplicación, para lo cual, debe conocer y aplicar:

- Las políticas de seguridad que garanticen un buen uso de los sistemas de información.
- La cláusula RGPD de confidencialidad y deber de secreto.
- Las medidas que permiten mantener un nivel de seguridad adecuado.

La aplicación de estas normas es de obligado cumplimiento para el personal, sin perjuicio del desempeño del resto de obligaciones que le pudieran ser de aplicación. Las políticas de Seguridad de la información se encuentran recogidas en el procedimiento [**SCGHCM - ENS - Política de seguridad**].

11. Delitos de descubrimiento y revelación de secretos empresariales

La **Política de privacidad corporativa,** que está disponible como anexo a este Código [**APR-BA-44-01 Política de privacidad corporativa**], establece que todas las personas de la organización, independientemente de su puesto de trabajo, están obligadas al secreto profesional en relación con toda la información que conozcan en el desempeño de su trabajo.

Por lo que, debe garantizarse la confidencialidad de toda la información que trata **GHCM/OPERADORA** por parte de todos sus trabajadores y colaboradores, siendo muy importante tener en cuenta que el deber de secreto se mantiene más allá de la finalización de la relación laboral. Por lo tanto, el deber de secreto no se extingue cuando finaliza la relación con la empresa, si no que se mantiene siempre: **no caduca**.

Para garantizar el cumplimiento de esta obligación, la empresa obtendrá de cada uno de sus empleados y colaboradores, de forma inexcusable, un compromiso estricto de confidencialidad contenido en el **acuerdo de confidencialidad y deber de secreto profesional** que se firma al inicio de la relación laboral del empleado o de colaboración con **GHCM/OPERADORA** de los socios de negocio.

12. Obligaciones contables y fiscales.

Los registros contables, estados financieros y demás documentación contable de la Sociedad Concesionaria deben reflejar correctamente la situación financiera y la realidad patrimonial de la empresa. **GHCM/OPERADORA** defienden la integridad fiscal, por lo que no se realizarán transacciones que tengan como finalidad la elusión fiscal o el falseamiento de la información contable o financiera, previniéndose el blanqueo de capitales.

Los empleados de **GHCM/OPERADORA** y demás personas obligadas realizarán un uso prudente del patrimonio de la empresa y velarán por que sus activos no sufran pérdida o menoscabo.

Los pagos y cobros que realice la Sociedad Concesionaria se ajustarán al procedimiento de pagos y tesorería **[PR-BA-03-01 Procedimiento de Pagos y Tesorería].** Como regla general, no podrá hacerse cobros o pagos en efectivo, salvo en supuestos de pagos de pequeña cuantía y de acuerdo con lo establecido en el procedimiento de compras **(PR-BA-03 Compras, cambios y evaluación de proveedores)**. Los pagos deberán estar debidamente justificados con facturas, contratos, pedidos, albaranes y el resto de los documentos y procedimientos establecidos. Queda expresamente prohibida la emisión de cheques al portador.

Los empleados de **GHCM/OPERADORA** prestarán especial atención a aquellos casos en los que se pongan de manifiesto indicios de la falta de integridad de las personas físicas o jurídicas con las que se contratan, para evitar y prevenir la intervención en eventuales operaciones de blanqueo de capitales provenientes de actividades delictivas o ilícitas.

13. Propiedad intelectual e industrial

GHCM/OPERADORA y sus empleados mantendrán especial cuidado y compromiso en la protección de los derechos de propiedad intelectual e industrial, propia y ajena, entre los que se incluyen los derechos, marcas, nombres de dominio, proyectos, programas, bases de datos y sistemas informáticos; conocimientos, procesos, tecnología, *"know how"*, equipos, manuales, videos o derechos sobre conocimientos técnicos especializados.

Los empleados de **GHCM/OPERADORA** respetarán los derechos de propiedad intelectual industrial de la empresa, y su utilización se hará exclusivamente en el desarrollo de su actividad en la misma, y se procederá a la devolución de todos los materiales en que tales derechos se soporten tan pronto como sean requeridos.

Igualmente se respetarán los derechos de propiedad intelectual e industrial que ostenten terceras personas ajenas a la Sociedad Concesionaria.

14. Política Desconexión Digital

Los cambios tecnológicos producidos en las últimas décadas han provocado modificaciones estructurales en el ámbito de las relaciones laborales. Estos cambios se deben fundamentalmente a la facilidad que, las nuevas tecnologías proporcionan a los empleados para acceder al trabajo, independientemente del lugar donde se encuentren físicamente y a la provisión de una conexión directa e inmediata de la empresa con ellos.

En este contexto, elementos tradicionales de la actividad laboral, como son el lugar de la prestación laboral y el tiempo de trabajo, se están viendo afectados por un fenómeno de "interconectividad digital" o conectividad permanente, que puede conllevar una inadecuada delimitación entre el tiempo de trabajo y el de descanso, afectando así al ámbito personal y familiar de los trabajadores y creando nuevos riesgos para la salud derivados de la sobreexposición tecnológica en el entorno laboral.

Por esta razón, y porque consideramos que los avances de la tecnología digital no deben dificultar una adecuada conciliación de la vida laboral y familiar de los trabajadores, ni suponer un riesgo para su salud, **GHCM/OPERADORA** ha diseñado una política interna con una serie de acciones y medidas preventivas para impulsar el derecho de los trabajadores a la desconexión digital una vez finalizada su jornada laboral, potenciando así el respeto a su tiempo de descanso, a su vida privada y familiar e impulsando hábitos saludables al respecto.

El derecho a la desconexión digital supone reconocer a los trabajadores el derecho a no conectarse a cualquier herramienta digital profesional (*smartphones,* portátiles, Internet, correo electrónico, WhatsApp, etc.) durante los periodos de descanso y vacaciones, con el fin último de controlar los límites de la jornada laboral y garantizar un tiempo de descanso al trabajador. El objetivo es garantizar el derecho al descanso, la conciliación de la vida personal y familiar, así como prevenir riesgos para la salud de los trabajadores.

A continuación, se definen los principios del ejercicio del derecho a la desconexión y se determinan una serie de medidas preventivas y acciones para promover el uso razonable de los instrumentos digitales, destinados a los trabajadores de la Sociedad Concesionaria.

14.1. Principios del derecho a la desconexión digital

- El derecho a la desconexión se reconoce al conjunto de trabajadores de **GHCM/OPERADORA.** El derecho del trabajador a "desconectar tecnológicamente" de su prestación laboral, se refiere al derecho de éste a no tener ningún contacto con herramientas digitales relacionadas con su trabajo durante el tiempo de descanso, fuera de su jornada de trabajo diario y/o en sus periodos de descanso semanal y/o anual. Para ello, se definen unas reglas de utilización y buen uso de las herramientas digitales (en las **Políticas de Seguridad de Información**), estableciendo además a título preventivo mecanismos para evitar las conexiones excesivas y proteger a los trabajadores que quieran ejercer este derecho.

- La desconexión digital no supone la prohibición de utilización por parte de los trabajadores de las herramientas digitales fuera del horario laboral, pues dicha desconexión es un derecho, no una obligación. En este sentido, corresponde al trabajador decidir si se conecta o no fuera de los horarios

habituales de trabajo. En todo caso, debe preocuparse de respetar los periodos mínimos de descanso diario, semanal y anual.

- El requerimiento de un trabajador fuera de su horario laboral está autorizado en el caso de que se produzca una situación de urgencia o gravedad. Estas situaciones excepcionales van desde la existencia de riesgos mayores o incidentes de tipo medioambiental (inundaciones, derrumbamientos, etc.), hasta incidencias relacionadas con virus informáticos, accidentes, riesgos sanitarios y otras cuestiones enmarcadas dentro del ámbito asistencial hospitalario que precisen de intervención urgente dentro del área de actividad de su competencia.
- Todos los empleados de la Concesionaria con riesgo de sufrir exposición a una prolongación excesiva de su jornada de trabajo y, por ende, al incremento de carga laboral o a la falta de desconexión con el trabajo durante su tiempo de descanso, deben ser sensibilizados y formados en el uso eficiente y responsable de las herramientas digitales.
- En el derecho a la desconexión, se debe tener en cuenta que es responsabilidad de la Concesionaria asegurar el servicio y satisfacer las necesidades de nuestro cliente. Sobre este derecho también incide la ocupación desarrollada y la posición jerárquica del trabajador.

14.2. Acciones y medidas para garantizar el derecho a la desconexión digital de los trabajadores.

A continuación, se recogen los mecanismos y medidas preventivas concretas que la empresa va a adoptar con relación al uso de dispositivos digitales fuera del horario laboral, para garantizar que los trabajadores puedan ejercer su derecho a la desconexión digital:

- Preferencia por creación de emails en modo borrador o uso del sistema de envío diferido si estamos fuera de la jornada laboral.
- De manera prioritaria, los mensajes (emails, WhatsApp, etc.) deben enviarse durante las horas habituales de trabajo. En el caso que los trabajadores decidan conectarse fuera de la jornada laboral, se recomienda que los mensajes se preparen en modo borrador, sin conexión o utilizar el sistema de envío diferido.
- Uso de respuestas automáticas en ausencia del trabajador
- Cuando un trabajador vaya a estar ausente por un periodo de tiempo superior a un día laborable, estará previsto una respuesta automática de ausencia para atender a sus interlocutores internos y externos, indicando quién es su interlocutor y cuáles son sus datos de contacto. Cada trabajador ha de definir un interlocutor, en función de su área de actividad y de la naturaleza y duración prevista de la ausencia.
- Buenas prácticas en el uso del correo electrónico:
  - Otras buenas prácticas, en el uso del correo para evitar la excesiva conexión tecnológica, son las siguientes:
  - Concienciar a los trabajadores en la reducción del envío de correos electrónicos y promover la comunicación directa.
  - Evitar poner en copia a personas que no están directamente vinculadas con el asunto.

C. COMPROMISO CON LOS DERECHOS HUMANOS

Este apartado del Código Ético recoge el compromiso de **GHCM/OPERADORA** con la protección de los Derechos Humanos, de conformidad con los más altos estándares internacionales, con el fin de que se apliquen en sus procedimientos, actividades empresariales y operaciones desarrolladas.

Los Derechos Humanos son derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua o cualquier otra condición. Estos derechos están institucionalizados principalmente en la Carta Internacional de Derechos Humanos de las Naciones Unidades, y en la Declaración de la O.I.T. (Organización Internaciones del Trabajo), relativa a los principios y derechos fundamentales en el trabajo y los ocho convenios fundamentales que ésta ha identificado.

15. Derechos Humanos

15.1. Alcance y ámbito de aplicación

Los principios de actuación de este compromiso son de aplicación directa a todas las actividades de gestión de GHCM/OPERADORA y serán la guía en materia de Derechos Humanos en las relaciones que la empresa establezca con sus empleados, clientes, proveedores y con la comunidad en la que desarrolla su actividad.

El objetivo consiste en minimizar el riesgo de infracción de los Derechos Humanos, a través del establecimiento de principios y pautas de actuación en materia de diligencia debida con los Derechos Humanos, que nos permita identificar, prevenir, mitigar y reparar posibles impactos negativos. En consecuencia, las actuaciones de la Sociedad Concesionaria incluirán:

- El establecimiento de compromisos.
- La asignación de responsabilidades.
- La corrección de errores y malas prácticas.
- La formación en la materia.

El Órgano de Cumplimiento Penal dispondrá de medios a su alcance para hacer cumplir los compromisos a este respecto, y garantizará su difusión en los contextos internos y externos de su actividad, principalmente, entre sus empleados y socios de negocio.

15.2. Compromisos con los empleados de la GHCM/OPERADORA

La relación de **GHCM/OPERADORA** con sus empleados y la de éstos entre sí se basará en el cumplimiento de los siguientes compromisos:

a. **Igualdad de oportunidades**: la organización promueve el desarrollo profesional y personal de todos sus empleados, asegurando la igualdad de oportunidades a través de su política de selección, gestión, promoción y desarrollo de los trabajadores, fundamentada en criterios objetivos de mérito y capacidad.

b. **Respeto a la diversidad y no discriminación**: los directivos de la Sociedad Concesionaria se comprometen a mantener el entorno de trabajo libre de toda discriminación. Bajo esta premisa **GHCM/OPERADORA** no tolerará ningún tipo de discriminación por razón de raza, nacionalidad, origen social, edad, sexo, discapacidad, estado civil, orientación social, ideología, opiniones políticas o sindicales, religión, estatus socioeconómico o cualquier otra condición personal, física o social.

c. **Seguridad y Salud laboral**: **GHCM/OPERADORA** se compromete a ofrecer a sus trabajadores y demás partes involucradas, un entorno de trabajo seguro y saludable, y a cumplir escrupulosamente la normativa aplicable en materia de salud laboral y PRL, que se apliquen en el desarrollo de sus actividades, así como a actualizar de manera permanente todas las medidas preventivas que correspondan. Además, la Sociedad Concesionaria se comprometerá a promover la difusión y refuerzo de una cultura de la seguridad, desarrollando la concienciación sobre el riesgo y fomentando el comportamiento responsable por parte de sus trabajadores, mediante sesiones de formación y entrega de información relativa a seguridad y salud laboral.

d. **Condiciones de trabajo justas y favorables**: **GHCM/OPERADORA** se compromete a mantener un entorno de trabajo positivo y respetuoso, rechazando toda forma de acoso, amenaza o intimidación en el lugar de trabajo. La política de remuneraciones de la Sociedad Concesionaria tiene en cuenta el principio de retribución justa del trabajo y respeta el principio de igualdad de remuneración entre trabajadores de distinto género por un trabajo de igual valor, basada en la evaluación objetiva del empleo. La remuneración mínima que reciben sus empleados nunca es inferior al mínimo recogido en los convenios colectivos y en la normativa laboral vigente. La Sociedad Concesionaria reconoce la importancia de la formación profesional para el desarrollo de las competencias y habilidades de sus trabajadores.

e. **Sensibilización de los trabajadores de GHCM/OPERADORA en materia de Derechos Humanos**: La Sociedad Concesionaria se compromete a difundir y hacer públicos sus compromisos en materia de Derechos Humanos, así como fomentar la realización de iniciativas de formación entre sus empleados en materia de ética, integridad y Derechos Humanos. Asimismo, se compromete a difundir esta política a proveedores, empresas subcontratadas y colaboradoras, promoviendo e incentivando que los diversos componentes de la cadena de valor desarrollen sus propios compromisos éticos, ya sea a través de sus propias políticas o suscribiendo la nuestra.

15.3. Compromisos con los clientes y proveedores

GHCM/OPERADORA exige a sus trabajadores el respeto a las personas, su dignidad y sus valores fundamentales, tal y como se recoge en este Código Ético. Además, se compromete a desarrollar su actividad basándose en una alta profesionalidad de sus trabajadores, que permita dar un servicio eficiente y ajustado a las necesidades de sus clientes y usuarios, enfocándose en la excelencia y calidad del servicio. La actividad de **GHCM/OPERADORA** se orienta al cliente, promoviendo relaciones de confianza, comprometiéndose, asimismo, a mantener con ellos una relación basada en los principios de transparencia, confidencialidad y no discriminación.

Además, se compromete a actuar con imparcialidad y objetividad en los procesos de selección de empresas subcontratadas, proveedores y colaboradores externos, aplicando criterio de calidad-coste y evitando la

colisión de sus intereses personales con los de la empresa, tal como se recoge en los procedimientos de homologación de proveedores y diligencia debida [**PR-BA-03 Compras, cambios y evaluación de proveedores, PR-BA-43 Procedimiento de diligencia debida**].

Asimismo, se asegura de la difusión y conocimiento de los compromisos adoptado por la Sociedad Concesionaria en relación con los Derecho Humanos, entre sus empresas subcontratadas, proveedores y colaboradores externos, así como la suscripción de los mismos y el establecimiento de mecanismos que permitan detectar malas prácticas en este ámbito.

Adicionalmente, a los efectos del cumplimiento de la presente Política, **GHCM/OPERADORA** cuenta con un procedimiento de reclamaciones, **PR-BA-05 Reclamaciones y satisfacción cliente,** en el cual se describen los procedimientos que se han de llevar a cabo en la atención al usuario.

15.4. Compromisos en relación con el entorno como parte de la comunidad

La Sociedad Concesionaria asume el compromiso de procurar al mayor respeto a los Derechos Humanos en el entorno y las comunidades en las que se desarrolla su actividad. Para ello, la Sociedad Concesionaria se compromete a desarrollar sus actividades conforme a:

- La competencia leal, evitando cualquier tipo de conducta y procedimiento en contra de la competencia.
- El cumplimiento de la normativa laboral y fiscal vigente.
- El respeto al medio ambiente en el desarrollo de las actividades, minimizando en cualquier caso los efectos negativos que, eventualmente, éstas pudieran ocasionar.
- Compromiso de actuación de forma sostenible, contribuyendo al desarrollo económico y social, promoviendo la contratación de trabajadores locales.

15.5. Implementación, cumplimiento y comunicación de la política de Derechos Humanos

La cultura de Derechos Humanos se integra en la empresa a través de acciones formativas para asegurar que todos los trabajadores de **GHCM/OPERADORA** comprendan adecuadamente el contenido de esta política. En su implementación, se tendrán en cuenta el Código Ético de Conducta aprobado por el Órgano de Cumplimiento Penal.

Asimismo, GHCM/OPERADORA analizará periódicamente los asuntos de Derechos Humanos relativos a su actividad e implantará procesos de debida diligencia de actividades y proyectos, para valorar el riesgo de incumplimiento, a partir de los cuales propondrá medidas de prevención o corrección de los impactos negativos que se pudiesen detectar.

Además, mantendrá y dará difusión de los mecanismos de comunicación o reclamación efectivos para que las personas directamente afectadas por sus operaciones puedan poner en su conocimiento cualquier situación de posible impacto en materia de Derechos Humanos.

En este sentido, los trabajadores de GHCM/OPERADORA tienen la obligación de poner en conocimiento cualquier posible incumplimiento de los compromisos recogidos en este protocolo, del que tengan conocimiento, así como de las demás directrices y pautas de conducta establecidas en el presente Código Ético.

Para ello, GHCM/OPERADORA dispone de un canal de ético de comunicación, dirigido a la recepción de notificaciones relacionadas con conductas o actividades irregulares que permite a los trabajadores remitir, con total confidencialidad, cualquier consulta sobre estas u otras cuestiones.

La Sociedad Concesionaria espera de todos sus trabajadores un alto nivel de compromiso en el cumplimiento de esta política. Cualquier incumplimiento podrá dar lugar, en su caso, a las correspondientes medidas disciplinarias.

15.6. Sistemas de supervisión y seguimiento

Corresponde al Órgano de Cumplimiento Penal la supervisión del cumplimiento de la Política de Derechos Humanos. Su seguimiento y evaluación se realiza a través de dicho órgano y a través del Canal de comunicación ético que permite comunicar las conductas irregulares o cualquier incumplimiento de las normas recogidas en el Código, a través de la dirección de correo: canaleticoghcm@targatis.com

Este órgano será el responsable de llevar a cabo los procesos de diligencia debida en el desarrollo de su actividad, analizando los indicadores e información que permitan comprender y evaluar los riesgos en materia de Derechos Humanos, así como la adopción de las medidas necesarias para prevenir y mitigar estos riesgos.

En este aspecto, se establecen unos mecanismos y procedimientos para minimizar el riesgo de malas prácticas relacionadas con los Derechos Humanos, entre las que se encuentran:

- Desarrollar iniciativas de concienciación en materia de ética, integridad y Derechos Humanos entre sus empleados.
- Promover e incentivar que los proveedores, empresas subcontratadas y empresa colaboradoras formalicen su compromiso con los Derechos Humanos y que, en el caso de no disponer de política propia en la materia, suscriban la de la Concesionaria.

Este compromiso con los Derechos Humanos será revisado anualmente para garantizar su adecuación y efectiva implantación. Todas las revisiones estarán sometidas a la aprobación del Órgano de Cumplimiento Penal de la Sociedad Concesionaria.

1. Objeto

En el desarrollo de la implementación del Sistema de Gestión de Cumplimiento Penal (en adelante, el "SGCP") se ha detectado la necesidad de definir y compilar la información referente a la Política de Privacidad Corporativa de la organización, que se encontraba disgregada, y así identificar los requisitos aplicables a la actividad de **GHCM/OPERADORA** y establecer el contenido y metodología aplicables.

2. Alcance y aspectos generales

La política se circunscribe a los empleados y colaboradores de **GHCM/OPERADORA.**
Se considera una violación de secretos empresariales:

2.1. La obtención de dichos secretos sin el consentimiento de su titular (acceso, apropiación o copia no autorizada de documentos, objetos, materiales, ficheros u otros soportes).
2.2. El incumplimiento del compromiso de confidencialidad adquirido por el trabajador con **GHCM/OPERADORA.**
2.3. Cualquier otra actuación que se considere contraria a las prácticas comerciales leales.

El deber de secreto resulta exigible, tanto durante la prestación de los servicios, como con posterioridad a la extinción de su relación con la empresa, ello con independencia de los motivos y forma en que haya tenido lugar dicha extinción.
Por lo tanto, el personal de **GHCM/OPERADORA** está obligado a respetar, en todo momento, tanto la confidencialidad de la información, incluidos los datos personales a los que tienen acceso los empleados en el marco de la relación laboral mantenida con la organización, así como la ley de secretos empresariales. En caso contrario, la organización podrá tomar las medidas legales que considere oportunas, incluyendo la adopción de medidas disciplinarias y, en todo caso, podrá ser causa de reclamación de indemnización por daños y perjuicios, así como, de haber mediado retribución por su revelación, uso o difusión, la exigencia de entrega de la misma, o de su valor equivalente, a la Empresa.

3. Desarrollo

3.1. Delitos de descubrimiento y revelación de secretos empresariales

La Política de privacidad corporativa establece que todas las personas de la organización, independientemente de su puesto de trabajo, están obligadas al secreto profesional en relación con toda la información que conozcan en el desempeño de su trabajo e infringir el deber de secreto, puede tener consecuencias laborales, civiles y penales.

Debe garantizarse la confidencialidad de toda la información que se trata en **GHCM/OPERADORA** por parte de todos sus trabajadores y colaboradores, siendo muy importante tener en cuenta que el deber de secreto se mantiene más allá de la finalización de la relación laboral. Por lo tanto, el deber de secreto no se extingue cuando finaliza la relación con la empresa, si no que se mantiene siempre: no caduca.

Para garantizar el cumplimiento de esta obligación, **GHCM/OPERADORA** como responsable, obtendrá de cada uno de sus empleados y colaboradores, de forma inexcusable, compromiso estricto de confidencialidad (**Cláusula de información y deber de secreto profesional**), que se firma al inicio de la relación laboral del empleado o colaborador de la Sociedad Concesionaria.
Se define como secreto empresarial, cualquier información o conocimiento (tecnológico, científico, industrial, comercial, organizativo o financiero), cualquiera que sea su soporte:

- Sea secreto, por lo tanto, no sea fácilmente accesible ni conocido.
- Tenga un valor empresaria real o comercial, por su carácter secreto.
- Ser objeto de medidas razonables para mantener su carácter secreto.

Desde listados de precios a tarifas, a listados de proveedores o clientes, a estrategias comerciales, protocolos, manuales e instrucciones técnicas, correspondencia, documentación o comunicaciones con los clientes, organigramas o funcionamiento interno de la empresa, datos financieros, presupuestos, la lista de información y documentación confidencial es extensa.
Por ello, la información que se entiende como secreto empresarial en la organización no puede ser copiada, entregada, revelada o facilitada por los empleados o directivos de **GHCM/OPERADORA** fuera de los cometidos propios de su actividad de trabajo y para los objetivos que se le hayan establecido o autorizado.
Actualmente, está en vigor la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que protege el secreto empresarial y establece un régimen de penalizaciones por no respetar el secreto empresarial por parte de los trabajadores. Queda al margen de la protección de esta ley, la información de escasa importancia, la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional y la información que es de conocimiento general o fácilmente accesible es los círculos en que normalmente se utilice el tipo de información en cuestión.
Se considera una violación de secretos empresariales la obtención de dichos secretos sin el consentimiento de su titular (acceso, apropiación o copia no autorizada de documentos, objetos, materiales, ficheros u otros soportes), el incumplimiento del compromiso de confidencialidad adquirido por el trabajador con la Sociedad Concesionaria o cualquier otra actuación que se considere contraria a las prácticas comerciales leales. Por lo tanto, los trabajadores de **GHCM/OPERADORA** están obligados a respetar la cláusula de confidencialidad, así como la ley de secretos empresariales. En caso contrario, la concesionaria podrá tomar las medidas legales oportunas, aplicar las sanciones disciplinarias pertinentes que pudieran corresponder de conformidad con la legislación vigente, sino también a reclamar al usuario los daños y perjuicios que la vulneración de este deber de confidencialidad pueda producir o que se deriven de ella.

Por lo que, tras la finalización de la relación profesional con la empresa por cualquier causa, el empleado deberá devolver todos los documentos, archivos y materiales que contengan información confidencial, incluidas las herramientas telemáticas que tengan en su poder, dispositivos digitales, sin poder reservarse para sí copia alguna ni extracto de los mismos. Asimismo, en caso de suspensión de la relación laboral, la empresa se reserva la facultad de solicitar a la persona trabajadora la devolución de los archivos, documentos, materiales y herramientas telemáticas que tenga en su poder.

3.2. Delitos contra la intimidad y allanamiento informático y el delito de daños informáticos.

GHCM/OPERADORA dispone de una serie de **Políticas de Seguridad de la información**, en las que se define el buen uso de los activos de la organización y del tratamiento de la información asociadas, incluyendo los datos de carácter personal.
Estas políticas son de aplicación general y nos remitimos a ellas, para su conocimiento en profundidad.
Todo el personal de **GHCM/OPERADORA** debe conocer esa normativa interna ya que afecta a los distintos recursos de la organización, como pueden ser:

- Los puestos de trabajo y sistemas de informáticos o aplicaciones establecidos para acceder a la información.
- Los servidores y entorno del sistema operativo en el que se encuentran los ficheros.
- La documentación impresa.

Para evitar comprometer las medidas de seguridad establecidas, no se podrán realizar las siguientes prácticas, salvo autorización del responsable de Sistemas de Información:

a) Cualquier uso para fines personales.
b) Instalar o modificar la configuración de software de los equipos (sistema operativo, programas instalados, etc.)
c) Realizar conexiones a redes o sistemas externos a la red propia.
d) Trasladar fuera de las instalaciones habituales de trabajo, equipos, información confidencial o datos de carácter personal, sea en formato automatizado o no; sin la correspondiente autorización y sin garantizar el nivel de seguridad correspondiente con anterioridad a la extracción.
e) Modificar o desactivar los mecanismos de seguridad para la protección de los recursos informáticos y de los sistemas de información de la organización.

El equipo informático, o estación de trabajo de cada usuario, tendrá una configuración fija en sus sistemas operativos y aplicaciones que, solamente, podrá ser cambiada bajo la autorización de la Dirección de la empresa y por el Departamento de informática. Igualmente, está absolutamente prohibida la instalación de cualquier programa, aplicación o utilidad informática o su supresión sin el consentimiento expreso o escrito de la Dirección o del área informática.

La instalación de dichos programas, aplicaciones o utilidades o su supresión deberá, una vez autorizada, ser llevada a cabo por el Departamento de informática.

- Se ha inhabilitado la instalación de programas informáticos por parte del usuario. La instalación debe siempre realizarse por el Departamento de informática, para asegurarse que se cumple con las medidas de seguridad requeridas y se cuenta con las garantías de soporte correspondientes. Su instalación y uso estará en función de las licencias adquiridas.
- El acceso a Internet debe responder únicamente a fines profesionales. Las conexiones que se produzcan a través de la red deben obedecer a fines propios del puesto de trabajo, con el propósito de obtener el mayor aprovechamiento de los recursos informáticos. El personal debe saber que en el ejercicio de sus funciones laborales representa a la organización por lo que su conducta debe reflejar la ética, profesionalidad, cortesía y responsabilidad correspondiente.
- Por motivos de seguridad y rendimiento, se informa que el Departamento de informática puede monitorizar el uso de Internet, tal y como se recoge en el artículo 20.3 del Estatuto de los Trabajadores.
- Las direcciones de correo electrónico con el dominio **GHCM/OPERADORA** son propiedad de la empresa y se considera un instrumento/herramienta de trabajo que debe ser utilizado sólo con fines relacionados con las funciones del trabajador. Por lo tanto, son herramientas de uso profesional y los usuarios autorizados son responsables del uso que se haga de los mismo. Se debe evitar cualquier práctica que pueda poner en riesgo el funcionamiento y buen uso del sistema.

3.3. Confidencialidad de la información.

Como ya se ha indicado anteriormente, tanto durante la vigencia de la relación laboral como después, el usuario se obliga a mantener la más estricta confidencialidad sobre cualquier información o datos a los que haya tenido acceso durante la vigencia de su relación laboral con la empresa, y que se refieran o estén relacionados en cualquier forma con la tecnología, cuentas, clientes, derechos de propiedad intelectual e industrial, "know-how", métodos, organización, datos personales, contratos o actividades de la empresa, o de cualquier persona o entidad que hubiera tenido contacto con las mismas (la "Información Confidencial").

En orden a garantizar dicha confidencialidad, el usuario únicamente tendrá acceso a la información confidencial que resulte necesaria para el desempeño de sus funciones, mediante la creación y asignación de perfiles de usuario, con sus correspondientes contraseñas de acceso.

- Es responsabilidad de cada usuario evitar que personas no autorizadas, inclusive compañeros de trabajo, tengan acceso a través del equipo informático asignado a la información contenida en el mismo o en la red, al que estas personas no tengan acceso autorizado. A tal efecto, al abandonar el puesto de trabajo (final de la jornada laboral, salida, pausa, descanso, reuniones...) el usuario

deberá apagar el equipo o bloquearlo, de forma que solamente pueda reanudarse la sesión mediante la introducción nuevamente de usuario y contraseña personal.

- Para una mejor conservación, organización, control y protección, todo documento informático relativo a la empresa deberá guardarse en el servidor, en el directorio designado por el departamento de informática, no pudiendo almacenarse en las unidades de disco duro u otro dispositivo, salo que exista autorización expresa por parte de la dirección de la empresa.
- Con carácter general, el uso de memorias USB, discos duros externos, no está autorizado. Por ello, aunque no están deshabilitados los puertos USB de los equipos informáticos, se limita su uso por parte de los usuarios a requerimiento específicos de comunicaciones con las partes interesadas, en concreto, con el IbSalut.
- No está permitido almacenar datos de carácter personal de los empleados en los ordenadores que la empresa les facilite, ni en ningún otro al que tengan acceso por su actividad profesional.

Todos los empleados de la Sociedad Concesionaria y demás personas obligadas respetarán de forma rigurosa las normas sobre protección de datos que se comunican en el Plan o Manual de Acogida.

1. Objeto

Dentro los usos sociales comúnmente aceptados en prácticas comerciales, el intercambio de regalos y gestos de cortesía juega un papel significativo, ya que culturalmente, estos se han considerado como una forma de fortalecimiento de las relaciones profesionales y personales.

Sin embargo, es imperativo que estos intercambios se realicen dentro de la legalidad y de la más estricta integridad y transparencia, respetando, en todo caso, los límites establecidos en la presente Política.

Desde SCGHCM/ OPERADORA promovemos activamente la prevención y la intolerancia frente a cualquier forma de soborno por lo que, esta Política ha sido desarrollada con el propósito de establecer pautas claras y éticas sobre cómo se deben abordar situaciones que involucren la recepción o entrega de regalos, favores o gestos de hospitalidad para evitar así, situaciones que puedan conducir a prácticas ilegales o antiéticas.

En ella no solo se establecen límites en términos de valor y frecuencia, sino que se define un marco de actuación en términos honestidad, responsabilidad, integridad, imparcialidad y transparencia que debe aplicarse en todas las transacciones de negocio, garantizando prácticas comerciales éticas que eviten conflictos de interés.

2. Alcance

Esta Política se aplica a todos los empleados, directivos, contratistas, proveedores y clientes, así como a cualquier otra parte interesada o socio de negocio que interactúe con **SCGHCM/ OPERADORA**.

Todos ellos, tienen la obligación de conocer y cumplir la presente Política, con independencia de la modalidad contractual que regule su relación jurídica o del puesto en el que desempeñen su trabajo.

En este sentido, esta Política no cubre todas las situaciones o cuestiones que puedan surgir, por lo que siempre se debe proceder con buen criterio y buscar asesoramiento de su superior inmediato o del Órgano de Compliance Penal.

3. Definiciones

- **Regalos**: cualquier obsequio, descuento, beneficio o transferencia de valor, ya sea tangible o intangible.
- **Favores**: cualquier acto que implica la realización de acciones específicas con intención de beneficiar o de dar u obtener un trato especial.
- **Agasajos y atenciones**: gestos, consideraciones de cortesía o expresiones de buena voluntad que por su naturaleza buscan establecer relaciones positivas.
- **Entretenimientos y Hospitalidades**: cualquier actividad recreativa, o de ocio, que suponga un beneficio con valor económico incluyendo, pero sin limitarse a, viajes, comidas, bebidas, alojamientos, espectáculos, eventos culturales o deportivos y asimilables.

- **Pagos de facilitación**: aquellos pagos realizados a funcionarios o personas encargadas de servicios públicos con el propósito de agilizar o facilitar trámites o procesos administrativos. La intención detrás de estos pagos suele ser obtener un tratamiento preferencial o acelerar procedimientos burocráticos y pueden socavar la transparencia y la equidad en la prestación de servicios públicos.
- **Contribuciones políticas**: donaciones de dinero, bienes, o servicios, realizadas por individuos, empresas u organizaciones a partidos políticos, candidatos políticos, comités de acción política (PAC) u otras entidades políticas.
- **Órgano de Compliance Penal (OCP)**: Es el Comité de Compliance del Sistema de Gestion de Compliance Penal de la Organización y que se encuentra regulado en el procedimiento PR-BA-40.

A efectos de la presente Política el término "Regalo", tanto en singular como plural, se entenderá en un sentido amplio, comprendiendo cualquier forma de beneficio, regalo, obsequio, agasajo, atención, favor, entretenimiento, hospitalidad y similares.

4. Principios generales

Queda expresamente prohibida, perseguida y sancionada cualquier forma de soborno o intento de influencia indebida realizada a través de cualquier medio, incluyendo sin limitarse a, regalos, obsequios, agasajos, atenciones, favores y hospitalidades.

En línea con lo anterior, se prohíbe categóricamente cualquier forma de soborno dirigida a autoridades, funcionarios públicos, empresas vinculadas a entidades gubernamentales a nivel nacional o internacional, así como a terceros con los que mantenga cualquier tipo de relación.

➢ Se **prohíbe** expresamente a los miembros de **SCGHCM/ OPERADORA**:

- Solicitar cualquier tipo de regalo en beneficio propio o de un tercero, de acuerdo con las disposiciones de la presente Política.
- La aceptación de regalos consistentes en dinero en efectivo, ayuda financiera personal, tarjetas regalo o cheques que permitan su uso como dinero en efectivo.
- La aceptación de regalos, agasajos, favores u hospitalidades para familiares.
- La aceptación de beneficios tales como promesas de empleo y asimilables, para uno mismo o un tercero.
- Realizar, ofrecer o prometer pagos de facilitación.
- Realizar, ofrecer o prometer contribuciones políticas. A este respecto, **SCGHCM/ OPERADORA** no se opone a que sus miembros realicen contribuciones políticas a título personal, siempre y cuando quede completamente claro que no lo hace en representación de **SCGHCM/ OPERADORA** ni con recursos de esta.
- El ofrecimiento, promesa o entrega de cualquier tipo de regalo, agasajo, favor y hospitalidad a cualquier parte interesada, tercero o socio de negocio, con la finalidad de obtener un beneficio para sí mismo, familiar o tercero.

Los empleados y demás miembros de la Organización no están autorizados a proporcionar, ofrecer, ni comprometerse con, la entrega de regalos o favores, ya sea de forma directa o indirecta, con la expectativa de recibir algún tipo de ventaja, preferencia o beneficio en retorno, ni en nombre propio ni en nombre de **SCGHCM/ OPERADORA**.

- De manera excepcional, se **permite** la recepción de regalos a los miembros de SCGHCM/ OPERADORA cuando:

- Sean recibidos de forma transparente y pública: para ello, quien lo recibe debe ponerlo en conocimiento de su superior inmediato que lo comunicará al Órgano de Compliance Penal (OCP).
- No correspondan, ni creen la impresión de corresponder, a tratos preferentes o de favor, o a la obtención de condiciones de negocio más ventajosas, ni de sobornos.
- Sean de buen gusto y respeten las políticas de la Organización y en especial el Código Ético de la misma, del que dicha Política forma parte.
- Sean infrecuentes.
- No superen la cantidad de 100€.
- Cuenten con la autorización del Órgano de Compliance Penal en el supuesto de que superen la cantidad establecida de 100€.

5. Valor económico del regalo

Cuando el valor del regalo supere, o se estime que podría superar la cantidad de 100€, éste no podrá aceptarse y deberá ponerse inmediatamente en conocimiento del superior jerárquico, quien lo comunicará al OCP que, teniendo en cuenta los principios de la presente Política, decidirá sobre si procede o no la aceptación de este.

En todo caso, se prohíbe la aceptación de regalos excesivos que puedan influir indebidamente en las decisiones comerciales, en cuyo caso, deberán ser rechazados o devueltos -según corresponda- poniéndose en conocimiento del superior jerárquico inmediatamente, quien deberá comunicarlo al OCP.

Cualquier incidencia o duda de interpretación surgida en relación con la ejecución y cumplimiento de esta Política deberá ser puesta en conocimiento del OCP a través del Canal Ético, en la dirección de correo electrónico canaleticoghcm@targatis.com o a través del enlace de la web corporativa https://ghcanmisses.es/canal-etico-de-comunicacion/ .

6. Pautas de actuación

Cualquier miembro de **SCGHCM/ OPERADORA** que reciba o se le haya ofrecido algún regalo debe ponerlo en conocimiento de su superior jerárquico, o del OCP, o a través del Canal Interno de Información disponible en la Organización.

En el caso de que se comunique al superior jerárquico, éste deberá ponerlo inmediatamente en conocimiento del OCP que, en caso de que supere o se estime que pudiera superar la cantidad de 100€, decidirá sobre si procede la aceptación o no del mismo.

Los integrantes de **SCGHCM/ OPERADORA** deberán rechazar cualquier tipo de regalo que no cumpla con los términos de la presente Política, poniendo dicho hecho en conocimiento de la Organización a través de los canales mencionados en la misma.

El OCP deberá asegurar el cumplimiento apropiado de esta Política. No obstante, la responsabilidad del cumplimiento de las normas y estándares éticos, así como del respeto de las políticas de la Organización, recae sobre toda la Organización y, por ende, en todos sus integrantes sin excepción.

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.

Cualquier regalo ofrecido o aceptado deberá ajustarse a los principios establecidos en el Código Ético, a la presente Política y demás principios recogidos en el Sistema de Gestión de Compliance Penal, así como en la legislación que pudiera resultar de aplicación sin que, en ningún caso, se puedan llevar a cabo actuaciones contrarias a las mismas. El incumplimiento podrá ser sancionado como muy grave de conformidad con el Régimen disciplinario en vigor.

7. Revisión

Esta Política será revisada periódicamente para asegurar su relevancia y eficacia, y se actualizará según sea necesario.

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.