Política de Seguridad de la información

Control del Documento

Título	Política de seguridad de la información
Documento	QINNOVATE-ORG.1
Fecha de creación	14/04/2026
Versión	1.0

Registro de cambios del Documento

Revisión	Descripción de la modificación	Fecha
00	Aprobación Inicial	14/04/2026
01		
02		
03		

1 Aprobación y entrada en vigor

La presente Política de Seguridad de la Información ha sido aprobada por la Dirección de **Q Innovate Consultores** en la fecha indicada en el apartado "*control de documento*", siendo efectiva desde su fecha de ratificación.

Este documento constituye el marco normativo de máximo nivel en la organización y mantendrá su vigencia de forma indefinida hasta que sea sustituido por una nueva versión que responda a cambios legales, técnicos o estratégicos de la entidad.

2 Introducción

La información y los servicios digitales representan los activos más críticos y sensibles de **Q Innovate Consultores**, constituyendo la infraestructura lógica sobre la que se asientan todos los procesos de negocio y la prestación de servicios de consultoría y tecnológicos. En el actual contexto de transformación digital, la organización reconoce que la información no es solo un recurso operativo, sino un bien estratégico cuya integridad, disponibilidad y confidencialidad deben ser preservadas de manera inalienable. La creciente sofisticación de los vectores de ataque y la persistencia de las amenazas en el ciberespacio imponen la necesidad de trascender las medidas de protección tradicionales, adoptando un marco de gobernanza robusto que garantice la resiliencia frente a incidentes que puedan comprometer la confianza de nuestros clientes y la continuidad de la entidad.

Esta Política de Seguridad nace como respuesta a este desafío, estableciendo una estrategia que se adapta dinámicamente a las condiciones del entorno y a la evolución de los riesgos sistémicos. Para ello, **Q Innovate Consultores** integra de manera armonizada las exigencias del Real Decreto 311/2022 (Esquema Nacional de Seguridad - ENS) y los estándares internacionales ISO/IEC 27001. Este enfoque normativo garantiza que la seguridad de la información sea una disciplina transversal, presente en todos los estratos de la pirámide organizacional: desde el nivel estratégico, donde se define la visión y el compromiso de la Dirección, pasando por los niveles tácticos de gestión, hasta alcanzar las operaciones técnicas más granulares. Se asume, por tanto, que la seguridad es una responsabilidad compartida que debe permear en la cultura corporativa de la organización y extenderse con el mismo rigor a toda la cadena de suministro, exigiendo a proveedores y socios tecnológicos niveles de cumplimiento equivalentes a los propios para evitar que terceros se conviertan en puntos de debilidad estructural.

Bajo esta premisa, la organización se compromete a que la seguridad TIC sea una parte integral de cada etapa del ciclo de vida de sus sistemas, desde su concepción y diseño

hasta su eventual retirada del servicio. Esto implica que la identificación de requisitos de seguridad y la valoración de sus costes asociados deben estar presentes en cada planificación, solicitud de oferta y proyecto técnico que emprenda la entidad. **Q Innovate Consultores** no solo busca proteger el perímetro tecnológico, sino poner al usuario y sus derechos como centro de la estrategia, implementando medidas específicas como la seudonimización y el cifrado avanzado para salvaguardar la privacidad y la información corporativa o registros sensibles de clientes y alumnos.

El objetivo prioritario de esta política es la transición hacia un modelo de defensa proactiva. Esto requiere una capacidad permanente de vigilancia para monitorizar y analizar vulnerabilidades en tiempo real, permitiendo una detección temprana de anomalías que facilite una respuesta rápida y eficiente ante ciberincidentes. La meta final es garantizar la prestación continuada de los servicios esenciales, minimizando los tiempos de recuperación y asegurando que cualquier interrupción tenga el menor impacto posible en nuestros clientes. En última instancia, esta introducción establece el firme compromiso de **Q Innovate Consultores** de actuar de forma preventiva y resiliente, consolidando un entorno digital seguro que respalde la excelencia en sus servicios.

3 Medidas de prevención, detección, respuesta y recuperación

La transformación digital de los servicios prestados por **Q Innovate Consultores**, así como la sensibilidad de la información asociada a los mismos, exige una gestión integral de la seguridad que trascienda la protección perimetral clásica. En este sentido, la organización adopta un modelo de seguridad basado en la proactividad, la vigilancia continua y la capacidad de reacción, estructurado en las fases de prevención, detección, respuesta y recuperación. El objetivo fundamental de este enfoque es garantizar que las amenazas sobre los sistemas de información no lleguen a materializarse o que, en caso de hacerlo, su impacto sea controlado, limitado y no comprometa la integridad de los datos ni la continuidad de los servicios de consultoría y corporativos.

Para alcanzar este nivel de resiliencia, **Q Innovate Consultores** despliega una estrategia de Defensa en Profundidad, constituyendo múltiples niveles de seguridad técnica, organizativa y física que interactúan de forma holística. Este modelo asegura que, ante el eventual fallo de una medida de control, existan capas adicionales capaces de mitigar el riesgo de forma independiente y coordinada. Esta postura de seguridad robusta permite el desarrollo cíclico y evolutivo de controles específicos, adaptándose con agilidad a las nuevas amenazas y a los cambios en la infraestructura tecnológica. De este modo, la seguridad se consolida como un proceso dinámico de mejora continua, alineado con las exigencias del Esquema Nacional de Seguridad (ENS) y los estándares de calidad de la

norma ISO/IEC 27001, garantizando que la protección de los activos de información sea un componente intrínseco e inseparable de la excelencia operativa de la entidad.

3.1 Prevención

Q Innovate Consultores implementará las medidas de seguridad y controles necesarios para evitar que incidentes afecten a la información o a los servicios. Para ello, se basa en una evaluación constante de amenazas y riesgos, asegurando que tanto las protecciones técnicas como las responsabilidades de todo el personal estén claramente definidas y documentadas. El objetivo es que la seguridad sea parte integral de cada proceso desde su inicio, minimizando cualquier posible vulnerabilidad.

3.2 Detección

Se monitorizará de manera continua la operación de sus sistemas para detectar cualquier anomalía o degradación en la prestación de los servicios. Dado que un incidente puede afectar rápidamente la disponibilidad, se establecen mecanismos de detección y análisis que alertarán a los responsables ante cualquier desviación significativa de los parámetros normales. Esta vigilancia constante es clave para supervisar la eficacia de las líneas de defensa y permitir una respuesta inmediata que minimice el impacto en la organización.

3.3 Respuesta

Despliega medidas de respuesta inmediata ante cualquier evento que afecte a sus servicios o información, garantizando una reacción adecuada que evite que el sistema sea comprometido en su conjunto. Esta capacidad de respuesta se basa en protocolos claros que definen qué acciones ejecutar, quién debe intervenir y cuándo es el momento preciso para actuar.

La organización designa puntos de contacto específicos para coordinar la comunicación de incidentes con otros departamentos, organismos y agentes del sector. Estos protocolos aseguran un intercambio fluido de información y la coordinación necesaria con los Equipos de Respuesta a Emergencias (CERT), permitiendo una gestión de crisis eficaz que minimice el impacto operativo y garantice la seguridad del entorno profesional.

4 Misión y objetivos

Nuestra misión y objetivo clave es proporcionar servicios de consultoría, asesoramiento técnico e implantación de sistemas de gestión, tanto en empresas privadas como en

Administraciones Públicas. Para ello, la Seguridad de la Información tiene como objetivo directo garantizar la prestación continuada de estos servicios y proteger la confidencialidad de los datos asociados, asegurando que la tecnología sea un soporte fiable y seguro para nuestros clientes.

5 Principios básicos de seguridad

La seguridad de la información se fundamenta en una serie de principios que guían todas las decisiones y acciones dentro de la organización. Estos principios garantizan que los servicios de consultoría y formación se desarrollen en un entorno digital íntegro y confiable:

- **Seguridad Integral:** La seguridad no se limita a la tecnología, sino que se aborda como un proceso global que involucra al personal, las instalaciones físicas, los procesos administrativos y la infraestructura técnica. Ningún elemento se gestiona de forma aislada.
- **Gestión basada en el riesgo:** La implementación de controles y medidas de protección es siempre proporcional a los riesgos identificados. Mediante evaluaciones periódicas, se priorizan las actuaciones sobre aquellas amenazas que podrían tener un mayor impacto en la continuidad de los servicios de la entidad.
- **Defensa en profundidad:** Se establece una estrategia multicapa donde existen diversos controles solapados. De este modo, si una medida de seguridad falla, existen otras capas adicionales capaces de impedir o mitigar el impacto del incidente.
- **Prevención, detección y respuesta:** El sistema de seguridad está diseñado para evitar incidentes, pero asume que el riesgo cero no existe. Por ello, se equilibra la inversión entre evitar ataques, detectarlos en tiempo real cuando ocurren y disponer de planes de respuesta ágiles para minimizar daños.
- **Responsabilidad diferenciada:** La seguridad es una responsabilidad compartida, pero con roles claramente asignados. Cada empleado o colaborador conoce sus obligaciones específicas y el alcance de su responsabilidad respecto al uso de la información y los sistemas de la entidad.
- **Mejora continua:** La seguridad no es un estado estático, sino un ciclo de revisión constante. **Q Innovate Consultores** se compromete a evaluar y actualizar regularmente sus políticas y herramientas para adaptarse a la evolución de las amenazas y a los cambios en el entorno tecnológico y social.

6 Objetivos de seguridad de la información

Los objetivos de seguridad de la información se definen como las metas estratégicas que permiten medir el éxito de esta Política. Estos objetivos no solo buscan proteger la tecnología, sino asegurar que la prestación de los servicios de consultoría, asesoramiento técnico e implantación de sistemas de gestión y la formación especializada se realicen bajo los más altos estándares de confianza:

- **Disponibilidad y Continuidad del Servicio:** El objetivo primordial es asegurar que los sistemas de información, aplicaciones y redes que soportan la actividad de consultoría estén operativos y accesibles cuando se necesiten. Se busca minimizar el impacto de posibles fallos técnicos o incidentes mediante infraestructuras resilientes y planes de contingencia que garanticen que la prestación del servicio no se vea interrumpida.
- **Confidencialidad y Privacidad de los Usuarios:** Dado el nivel medio de sensibilidad de los datos gestionados en el ámbito de la consultoría y formación, la organización se marca como objetivo crítico que la información solo sea accesible por personal debidamente autorizado. Esto implica el uso de controles de acceso granulares y técnicas de protección que impidan la divulgación no autorizada de la información confidencial y datos personales de clientes y alumnos.
- **Integridad y Exactitud de la Información:** Se garantiza que la información almacenada y procesada sea veraz, exacta y completa. El objetivo es evitar cualquier alteración malintencionada o accidental de los registros de servicio, expedientes de alumnos o datos de gestión, asegurando que las decisiones tomadas por los profesionales se basen siempre en datos fiables.
- **Cumplimiento Normativo Transversal:** La organización asume el compromiso de cumplir de forma estricta con el marco legal vigente, así como con los requisitos contractuales adquiridos con administraciones públicas y terceros. Este objetivo incluye la adaptación constante a la normativa de protección de datos y a las exigencias de seguridad específicas de los servicios de consultoría y sistemas de gestión.
- **Capacitación y Compromiso del Capital Humano:** Se establece como meta que todo el personal, independientemente de su rol, posea los conocimientos necesarios para identificar riesgos básicos y aplicar medidas de protección en su desempeño diario. La seguridad se integra como una competencia más del puesto de trabajo, reduciendo la probabilidad de incidentes causados por errores humanos o falta de información.
- **Gestión Eficaz de Incidentes y Resiliencia:** El objetivo final es fortalecer la capacidad de detección temprana y respuesta ante amenazas. Se busca reducir el

tiempo de permanencia de cualquier incidente en el sistema y asegurar una recuperación ágil que restablezca la normalidad operativa con las menores consecuencias posibles para los usuarios y la reputación de la entidad.

7 Alcance

La presente Política de Seguridad de la Información (PSI) se aplica a todos los sistemas de información de **Q Innovate Consultores** relacionados con la prestación de sus servicios de consultoría, asesoramiento, implantación de sistemas y formación. Su cumplimiento es obligatorio para todas las personas con acceso autorizado a dichos sistemas, independientemente de su relación jurídica o naturaleza profesional. Todos los usuarios tienen el deber de conocer y acatar tanto esta PSI como su normativa derivada, siendo responsabilidad del Comité de Seguridad proveer los recursos y medios necesarios para garantizar su cumplimiento efectivo en toda la organización.

8 Marco normativo

Q Innovate Consultores cuenta con su Sede Central Jerez de la Frontera, provincia de Cádiz y Delegación en Málaga, pero ofrece sus servicios a lo largo de toda España, por lo que el marco normativo aplicable será el de obligado cumplimiento nacional.

Actualmente, se contempla el **RGPD** (Reglamento General de Protección de Datos) y la **LOPDGDD** (Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales) a nivel español, así como la normativa y leyes específicas de aplicación para los servicios de asesoramiento técnico, implantación de sistemas de gestión y formación que **Q Innovate Consultores** ofrece a sus clientes.

Por otro lado, **Q Innovate Consultores**, cuenta con un "*listado de requisitos legales aplicables*" a su actividad en materia de seguridad de la información, ciberseguridad, calidad y medioambiente, donde se identifican los requisitos legales aplicables y la evaluación de su cumplimiento.

9 Directrices del Sistema de Gestión de Seguridad de la Información

La estructuración, gestión y acceso a la información que forma parte del sistema de **Q Innovate Consultores** se somete a las premisas, principios y requisitos descritos en esta PSI. En concreto, el sistema de gestión se rige por las siguientes directrices:

- **Calificación de la información y servicios:** La información y los servicios se calificarán basándose en la normativa aplicable y en niveles que consideren su valor, sensibilidad y la confidencialidad requerida, siempre bajo los criterios aprobados por la dirección.
- **Gestión documentada y formal:** Se desarrollará un sistema de gestión de seguridad plenamente documentado y alineado con los requisitos de la normativa vigente. Este sistema estará sujeto a un proceso de aprobación formal, con revisiones y actualizaciones periódicas para asegurar su vigencia.
- **Proporcionalidad de las medidas:** La calificación de los activos, junto con los resultados de las evaluaciones de riesgo que se realicen, modularán la intensidad y el tipo de medidas de seguridad que deberán aplicarse en cada caso.
- **Alineación con objetivos estratégicos:** Los criterios de seguridad tendrán en cuenta la capacidad de la organización para lograr sus objetivos, la protección de sus bienes, el cumplimiento de sus obligaciones en la prestación de servicios de consultoría y el respeto estricto a la legalidad y los derechos de los usuarios.
- **Defensa multicapa:** Se establecerán medidas de seguridad en todas las capas que intervienen en el tratamiento de la información, abarcando controles de carácter organizativo, físico y lógico para garantizar una protección integral.
- **Capacitación del capital humano:** Todo el personal será debidamente capacitado e informado sobre sus deberes y obligaciones específicas en materia de seguridad de la información, asegurando que la cultura de seguridad sea parte del desempeño diario.
- **Deber de confidencialidad y secreto:** Todas las personas que manejen información no pública tienen la obligación estricta de mantener la confidencialidad y el secreto profesional. Esta obligación subsistirá de forma indefinida incluso tras la finalización de su vínculo jurídico con **Q Innovate Consultores.**

10 Organización de la seguridad de la información

10.1 Criterios utilizados

La arquitectura organizativa de la seguridad en **Q Innovate Consultores** se fundamenta en un modelo de gobernanza alineado estrictamente con el Real Decreto 311/2022 (Esquema Nacional de Seguridad) y los requisitos internacionales de la norma ISO/IEC 27001. Esta estructura constituye un sistema de gestión robusto basado en los siguientes criterios:

- La seguridad se define como un compromiso transversal que vincula a todos los miembros de la organización. **Q Innovate Consultores** garantiza que el ciclo de vida del sistema de seguridad sea comprendido y ejecutado por toda la plantilla como un proceso de mejora continua.
- Siguiendo el artículo 11 del ENS y los controles de la ISO 27001, se formalizan roles diferenciados: Responsable del Servicio, de la Información, de la Seguridad y del Sistema. Esta separación asegura que la supervisión de la seguridad sea independiente de la gestión operativa, evitando conflictos de interés.
- Se establece una estructura de mando estratégica para la toma de decisiones críticas, permitiendo la delegación de funciones en órganos especializados y garantizando canales formales para la resolución de cualquier discrepancia técnica o táctica.
- El eje central es el Comité de Seguridad de la Información. Este órgano colegiado asume la dirección estratégica y está presidido por una figura con autoridad ejecutiva que asume la responsabilidad formal de las políticas adoptadas.

10.2 Modelo de gobernanza

Se aplica un modelo de gobernanza centralizado que garantiza la unidad de mando y la cohesión en la protección de sus activos.

Esta estructura define una asignación inequívoca de competencias en todos los niveles jerárquicos, asegurando la separación de funciones exigida por la ISO 27001 y el ENS.

El modelo se integra en el organigrama de la entidad, estableciendo líneas claras de autoridad y responsabilidad que vinculan la operativa técnica con la dirección estratégica, garantizando así una supervisión continua de la seguridad en todos los servicios de la organización.

10.3 Funciones y responsabilidades

Bajo el marco del ENS y la norma ISO 27001, los roles y órganos de seguridad en **Q Innovate Consultores** se despliegan estratégicamente en todos los niveles jerárquicos, vinculando la alta dirección con las áreas operativas y técnicas. La organización procederá a la designación formal de los responsables necesarios, revisando dichos nombramientos cada dos años o ante cualquier vacante, para garantizar la continuidad y actualización del sistema. Estos responsables asumen las facultades necesarias para liderar la gestión integral de la seguridad, abarcando la protección operativa, la implementación de medidas técnicas, el análisis de riesgos y la respuesta ante incidentes para asegurar la resiliencia de la entidad. Asimismo, sus funciones incluyen el impulso de la mejora continua y la capacitación del personal, asegurando que la cultura de seguridad impregne todos los departamentos de la consultora.

Dentro de esta estructura, el Responsable de la Información tiene la potestad de definir los requisitos de seguridad de los datos tratados y determinar los niveles de criticidad de los mismos. Por su parte, el Responsable del Servicio determina los requisitos de seguridad de los servicios prestados, asegurando que las medidas aplicadas sean proporcionales a las necesidades de los clientes. El Responsable de Seguridad es la figura encargada de supervisar la implantación de las medidas técnicas y organizativas, velando por el cumplimiento de la presente PSI, mientras que el Responsable del Sistema asume la responsabilidad de la explotación y mantenimiento técnico de los activos de información.

Por último, todo el personal, clientes y proveedores de **Q Innovate Consultores** tienen la obligación de cumplir con las normas de seguridad establecidas, custodiar sus credenciales y reportar de forma inmediata cualquier incidente o debilidad detectada en el desempeño de sus funciones profesionales.

10.3.1 Responsable de la Información y Responsable del Servicio

Las figuras del Responsable de la Información y del Responsable del Servicio en **Q Innovate Consultores** pueden recaer en una misma persona física o en un órgano colegiado, asumiendo la competencia de determinar los requisitos de seguridad de los activos y servicios bajo su tutela. Su labor es estratégica, ya que actúan como los garantes de que la información tratada y los servicios de consultoría prestados cuenten con el nivel de protección adecuado conforme a la normativa vigente.

Entre sus funciones principales destaca la valoración de la información y los servicios, estableciendo los requisitos de seguridad específicos y dictaminando sobre los derechos de acceso necesarios para cada perfil. Asimismo, tienen la potestad de aceptar los niveles de riesgo residual y la obligación de comunicar de forma proactiva al Responsable de Seguridad cualquier variación en el inventario de activos, especialmente ante la

incorporación de nuevos servicios o categorías de información. En última instancia, son los encargados de evaluar el impacto que una posible indisponibilidad de los sistemas tendría sobre la continuidad de las actividades de **Q Innovate Consultores**, garantizando que la resiliencia operativa esté alineada con los objetivos de la organización y las expectativas de los clientes.

10.3.2 Responsable de Seguridad

El Responsable de Seguridad en **Q Innovate Consultores** asume la autoridad para determinar las decisiones necesarias que satisfagan los requisitos de seguridad de la información y de los servicios, supervisando directamente la implantación de las medidas técnicas y organizativas para garantizar su eficacia. Este rol ejerce el liderazgo estratégico de la seguridad y dirige las operaciones tácticas, actuando con total independencia jerárquica y funcional respecto al Responsable del Sistema. Esta segregación de funciones es imperativa para evitar conflictos de interés, asegurando que el Responsable de Seguridad no tenga responsabilidades directas sobre la prestación de servicios TIC ni sobre la explotación operativa de los sistemas. Solo de forma excepcional, y bajo autorización expresa del máximo órgano de gobierno ante la ausencia de recursos, podrían converger funciones bajo medidas compensatorias estrictas que garanticen la diferenciación de responsabilidades.

En el ejercicio de sus facultades, el Responsable de Seguridad dirige la oficina técnica de seguridad y actúa como el nexo de reporte principal ante el Comité de Seguridad. Entre sus funciones críticas se encuentra la validación y verificación constante del nivel de seguridad de la información manejada, promoviendo de forma proactiva la formación y concienciación de toda la plantilla. Es responsable de designar a los ejecutores de los procesos de análisis de riesgos, así como de desarrollar, documentar y aprobar formalmente la Declaración de Aplicabilidad. Asimismo, determina las configuraciones de seguridad necesarias y supervisa que el personal técnico elabore y custodie debidamente la documentación del sistema. Tiene la capacidad de implementar medidas adicionales o compensatorias a las requeridas por el ENS, considerando siempre el estado de la tecnología, la naturaleza de la información tratada y los riesgos específicos a los que se exponen los sistemas de **Q Innovate Consultores.**

Su labor se extiende al asesoramiento estratégico para la valoración de los sistemas y la determinación de sus categorías de seguridad, participando activamente en la elaboración de los planes de mejora y de continuidad de negocio. Gestiona íntegramente las revisiones externas e internas, los procesos de certificación bajo las normas de aplicación y eleva al Comité de Seguridad cualquier cambio estructural o requisito de inversión. Además, ostenta la competencia para aprobar los procedimientos operativos del mapa normativo y coordinar con el CSIRT de referencia o las autoridades de control cualquier incidente con impacto significativo. En estos casos, será el encargado de gestionar la comunicación de crisis y

notificar a los clientes y partes interesadas sobre las medidas adoptadas frente a ciberamenazas.

Finalmente, aunque el Responsable de Seguridad puede delegar funciones operativas en posiciones intermedias de la estructura orgánica, mantiene de forma indelegable la responsabilidad sobre la normativa, el seguimiento de la mejora del sistema, la conformidad del mismo, la aprobación de medidas compensatorias y la ejecución del análisis de riesgos. También conserva la dirección del análisis del ciclo de vida de los componentes y la validación de las auditorías técnicas, integrando si fuera necesario funciones de seguridad derivadas de normativas sectoriales específicas para asegurar que **Q Innovate** mantenga un blindaje integral de su activo más valioso: la información.

10.3.3 Responsable del Sistema

El Responsable del Sistema en **Q Innovate Consultores** asume la competencia de implantar la seguridad técnica y supervisar la operación diaria de la infraestructura, garantizando que el ciclo de vida de los sistemas de información, desde su especificación e instalación hasta su mantenimiento y verificación, se desarrolle bajo estándares de máxima eficiencia. Este rol ostenta la facultad de desarrollar sus cometidos directamente o mediante el apoyo de terceros especializados en ciberseguridad, pudiendo delegar funciones operativas en administradores u operadores bajo su cargo.

Asimismo, cuenta con la capacidad de apoyarse en servicios externos de monitorización y vigilancia activa para fortalecer las capacidades de detección y respuesta ante amenazas en tiempo real.

Sus funciones operativas se ejecutan en estrecha colaboración con el Responsable de Seguridad, centrando su actividad en la definición de la topología del sistema, la gestión de los criterios de uso de los servicios y la implantación efectiva de las medidas técnicas derivadas de los planes de tratamiento de riesgos. Como garante de la integridad tecnológica, el Responsable del Sistema tiene la potestad de detener el acceso a la información o la prestación de un servicio si tiene constancia de que existen deficiencias graves que comprometan la seguridad. Además, es responsable de asegurar que cualquier dispositivo que abandone las instalaciones de la entidad mantenga las configuraciones de seguridad necesarias conforme a la criticidad de la información que maneja, analizando de forma proactiva las conclusiones de las auditorías y revisiones internas para proponer mejoras en la arquitectura técnica.

En su dimensión como administrador de la seguridad del sistema, se encarga de la gestión, configuración y actualización del hardware y software, así como del control estricto de las autorizaciones y privilegios concedidos a los usuarios. Su labor incluye la monitorización constante de la actividad para asegurar la correspondencia entre las acciones ejecutadas y las autorizadas, garantizando que todos los procedimientos operativos se apliquen con rigor. Ante cualquier anomalía, compromiso o vulnerabilidad detectada, el Responsable del

Sistema informará de inmediato al Responsable de Seguridad, colaborando activamente en la investigación y resolución de incidentes desde su detección inicial hasta su cierre definitivo.

Finalmente, el Responsable del Sistema tiene la facultad de designar responsables delegados en función de la complejidad de los proyectos, manteniendo la supervisión directa sobre áreas clave como la ciberinteligencia, la gestión de bastionado (hardening), el parcheado de sistemas y la interconexión de redes. Esta estructura permite a **Q Innovate Consultores** mantener un entorno tecnológico resiliente, donde la gestión de cambios, las entradas en producción y la vigilancia activa se ejecutan con una trazabilidad absoluta y bajo el cumplimiento estricto del marco normativo de la ISO 27001 y el ENS.

10.3.4 Delegado de protección de datos

El Delegado de Protección de Datos actúa como el garante del cumplimiento normativo en materia de privacidad dentro de **Q Innovate Consultores**, ejerciendo sus funciones con total independencia técnica y reportando directamente a la Alta Dirección.

Su responsabilidad principal consiste en asesorar a la organización sobre las obligaciones derivadas del RGPD y la LOPDGDD, supervisando la implementación de las políticas de tratamiento de datos personales y colaborando en la realización de evaluaciones de impacto cuando la naturaleza de los servicios lo requiera. Asimismo, actúa como el punto de contacto fundamental para los interesados y la Agencia Española de Protección de Datos (AEPD), trabajando en estrecha coordinación con el Responsable de Seguridad para asegurar que las medidas técnicas y organizativas adoptadas protejan eficazmente los derechos y libertades de las personas físicas.

10.3.5 Comité de seguridad TIC (COMSEGTIC)

El Comité de Seguridad TIC se constituye como el máximo órgano colegiado especializado en la gobernanza de la seguridad de la información dentro de **Q Innovate Consultores**. Está integrado por los perfiles con mayor capacidad de decisión estratégica y técnica, incluyendo la Presidencia, el Responsable de Seguridad, el Responsable del Sistema y representantes de la alta dirección. Asimismo, el Secretario/a del comité gestionará las convocatorias y actas, pudiendo invitar a asesores externos, especialistas en ciberseguridad o al Delegado de Protección de Datos para garantizar que las decisiones estén alineadas con el marco legal y el estado de la tecnología.

Las atribuciones del COMSEGTIC se despliegan en cinco ejes fundamentales. En el ámbito de la coordinación y estrategia, el comité elabora la hoja de ruta global de seguridad, prioriza los recursos, resuelve conflictos de responsabilidad entre departamentos y promueve la integración de marcos de gobernanza. En cuanto al desarrollo normativo y gestión de

riesgos, se encarga de proponer e innovar en la normativa interna, aprobar la Declaración de Aplicabilidad y realizar el seguimiento de los planes de tratamiento de riesgos, validando los niveles de riesgo residual aceptables para la organización.

Respecto a la conformidad y mejora continua, el comité aprueba los planes de auditoría, se mantiene actualizado sobre los procesos de certificación y gestiona los resultados de las revisiones para impulsar el ciclo de mejora. En el área de formación y resiliencia, es el responsable de dotar de recursos y aprobar el plan anual de sensibilización, así como de liderar la respuesta ante incidentes críticos, coordinando la comunicación con autoridades competentes y el CSIRT de referencia. Finalmente, potencia la vigilancia activa, promoviendo servicios de alerta temprana y monitorización de la infraestructura para asegurar una postura de seguridad sólida basada en la ciberinteligencia.

El funcionamiento del COMSEGTIC se rige por la presente PSI y su propio reglamento interno. Para garantizar un seguimiento eficaz de las acciones estratégicas, el comité se reunirá con carácter ordinario al menos una vez al trimestre durante fases de despliegue operativo, y con un mínimo de dos veces al año para funciones de mantenimiento y mejora continua. Las sesiones serán convocadas por la Presidencia y los acuerdos se adoptarán por consenso de sus miembros permanentes, asegurando que cada decisión cuente con el respaldo técnico y directivo necesario para su correcta ejecución en toda la estructura de **Q Innovate Consultores.**

10.3.6 Otros roles o responsabilidades

Q Innovate Consultores podrá designar roles de seguridad adicionales siempre que sea necesario por imperativo legal o debido a la entrada en vigor de normativas particulares que detallen obligaciones específicas para la organización.

Estas figuras se integrarán en la estructura de gobernanza existente, asumiendo las funciones de supervisión o control que la legislación vigente determine en cada momento.

De igual modo, la Dirección podrá crear figuras delegadas o grupos de trabajo temporales para la gestión de proyectos críticos o situaciones de contingencia que requieran una especialización técnica concreta. Todos estos roles adicionales actuarán bajo los principios de responsabilidad y confidencialidad establecidos en este documento, asegurando que cualquier nueva competencia asignada esté perfectamente alineada con los objetivos generales de protección de la entidad.

10.4 Procedimiento de designación

La designación de los roles estratégicos de seguridad que incluyen al Responsable de la Información, al Responsable del Servicio, al Responsable de Seguridad y al Responsable del Sistema se formalizará mediante un nombramiento emitido por la Dirección de **Q**

Innovate Consultores, previa propuesta del Comité de Seguridad TIC. Este proceso garantiza que la estructura de gobernanza cuente con el respaldo de la alta dirección y la idoneidad técnica necesaria.

La revisión de estos cargos se realizará con una periodicidad de dos años, o bien cuando el puesto quede vacante por cambios en la estructura organizativa. Los criterios fundamentales para la designación o renovación de estas figuras se basan en:

- Evaluación de las habilidades y destrezas actuales dentro de la organización.
- Correspondencia entre el cargo operativo que desempeña el empleado y las responsabilidades asignadas en el marco de la seguridad.
- Valoración de la estabilidad del empleado en la empresa para asegurar una gestión a largo plazo.
- Capacidad real de la persona para asumir las funciones del cargo sin menoscabo de sus otras responsabilidades.
- Propuesta formal del Comité y ratificación final por parte de la Dirección de la empresa.

Por su parte, el Delegado de Protección de Datos, dada su condición frecuente de colaborador externo, será nombrado bajo el mismo procedimiento de propuesta y aprobación, aunque su vigencia se someterá a una revisión anual. En este caso, la continuidad de su designación estará sujeta a la vigencia del contrato de servicios profesionales y a la calidad del soporte prestado por la entidad externa, garantizando en todo momento que el perfil asignado cumple con los requisitos de independencia y especialización exigidos por la normativa vigente.

11 Datos personales

Q Innovate Consultores, en su condición de responsable del tratamiento, trata los datos personales conforme a los principios y obligaciones establecidos en el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD). La organización asume el compromiso de respetar el derecho fundamental a la protección de datos, la intimidad y el resto de libertades reconocidas en la Constitución y los tratados internacionales, asegurando que toda actividad de tratamiento se realice bajo criterios de licitud y transparencia.

Para garantizar el control de los interesados sobre su propia información, la entidad pone a su disposición información detallada sobre el uso de sus datos y facilita canales específicos para el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad. Estos mecanismos aseguran que cualquier persona afectada pueda gestionar su privacidad de forma ágil y efectiva ante el responsable.

Como refuerzo a esta estructura de cumplimiento, **Q Innovate Consultores** ha designado y registrado ante la autoridad de control un Delegado de Protección de Datos (DPD). Esta figura actúa de manera independiente y especializada, asesorando a la dirección en sus obligaciones legales y supervisando de forma constante las actuaciones internas. El DPD constituye el punto de enlace fundamental para atender tanto las consultas de los interesados como los requerimientos de la Agencia Española de Protección de Datos (AEPD), consolidando así un modelo de gestión basado en la responsabilidad proactiva.

12 Obligaciones del personal

Todas las personas que utilicen la información, los servicios o los sistemas de tratamiento integrados en el alcance de esta política tienen la obligación de conocer y respetar su contenido, así como el marco normativo de desarrollo que se apruebe para su cumplimiento. La responsabilidad individual es un pilar fundamental de la seguridad de la organización, por lo que el deber de protección se extiende a todos los niveles de la estructura de **Q Innovate Consultores**.

Como parte de estas obligaciones, el personal participará en sesiones de concienciación en materia de seguridad y protección de datos con una periodicidad mínima de una vez al año. La entidad mantendrá un programa de sensibilización continua diseñado para atender a toda la plantilla, prestando especial atención a las personas de nueva incorporación, quienes deberán ser instruidas en las normas de seguridad desde el inicio de su actividad profesional.

Por otra parte, quienes asuman responsabilidades específicas en el uso, operación o administración de sistemas de información recibirán formación técnica especializada para el manejo seguro de dichas infraestructuras. Esta capacitación tendrá carácter obligatorio y deberá completarse con anterioridad a la asunción de cualquier responsabilidad, aplicándose tanto en nuevas contrataciones como en cambios de puesto o modificaciones en las funciones asignadas. De este modo, se asegura que todo perfil con acceso a activos críticos posea las competencias necesarias para mitigar riesgos y aplicar los controles de seguridad de manera efectiva.

13 Gestión de riesgos

Todos los sistemas de información de **Q Innovate Consultores** están sujetos a un proceso continuo de gestión de riesgos con el objetivo de evaluar las amenazas a las que están expuestos y determinar el impacto potencial sobre la organización. Este análisis es una pieza fundamental para la toma de decisiones estratégicas y se repetirá obligatoriamente en los siguientes casos:

- Al menos una vez al año para asegurar la vigencia de los controles.
- Cuando se produzcan modificaciones sustanciales en la información manejada o en los servicios prestados.
- Tras la ocurrencia de un incidente grave de seguridad o ante la detección de vulnerabilidades que comprometan el sistema.

El Responsable de Seguridad tiene la competencia de liderar la ejecución de estos análisis, así como de identificar carencias y debilidades que deban ser puestas en conocimiento del Comité de Seguridad TIC. Por su parte, el Comité se encargará de dinamizar la disponibilidad de recursos necesarios para atender las necesidades detectadas, promoviendo inversiones de carácter horizontal que fortalezcan la infraestructura de la entidad.

El proceso de gestión de riesgos se desarrolla en tres fases principales: la categorización de los sistemas, el análisis de riesgos propiamente dicho y, finalmente, la selección de medidas de seguridad. Para la ejecución de estas fases, **Q Innovate Consultores** empleará con carácter general metodologías de reconocido prestigio en el ámbito de la seguridad de la información. La elección de las salvaguardas será siempre proporcional a los riesgos identificados y estará debidamente justificada, garantizando un equilibrio óptimo entre la protección de los activos y la operatividad de los servicios.

14 Notificación de incidentes

De conformidad con lo dispuesto en el Esquema Nacional de Seguridad, **Q Innovate Consultores** dispone de procedimientos formales para la gestión de incidentes de seguridad, alineados con las instrucciones técnicas correspondientes y la normativa sectorial vigente. La organización cuenta con mecanismos de detección, criterios de clasificación y protocolos de análisis y resolución que aseguran una respuesta eficaz ante cualquier evento que comprometa la integridad de sus sistemas. Para garantizar una gestión integral, se definen cauces claros para informar a las partes interesadas y se mantiene un registro exhaustivo de todas las actuaciones e intervenciones realizadas durante la vida del incidente.

En cumplimiento de sus obligaciones normativas, la entidad desplegará las medidas necesarias para notificar al Centro Criptológico Nacional (CCN) aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada o en la prestación de los servicios, atendiendo siempre a la categorización de los sistemas afectados. Asimismo, se mantendrá una interacción constante con los CERT-CSIRT de referencia, siguiendo sus directrices y adoptando las medidas requeridas por los equipos de respuesta de las autoridades competentes. El personal de la organización tiene el deber de reportar cualquier anomalía detectada a través de los procedimientos internos,

permitiendo que el Responsable de Seguridad active los protocolos de respuesta y reporte externo de manera ágil, asegurando así la trazabilidad y el aprendizaje continuo para reforzar la robustez de la infraestructura tecnológica de la compañía.

15 Desarrollo de la política de seguridad de la información

La presente Política de Seguridad de la Información (PSI) se complementa mediante un cuerpo normativo dinámico que incluye normativas, procedimientos técnicos, informes y registros. Este desarrollo se articula en tres niveles jerárquicos según su ámbito de aplicación, detalle técnico y obligatoriedad:

- **Primer nivel normativo:** Constituido por la presente PSI, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a toda la organización. Su aprobación corresponde a la Dirección de **Q Innovate Consultores**.
- **Segundo nivel normativo:** Integrado por las normas de seguridad específicas que desarrollan los principios establecidos en el nivel superior.
- **Tercer nivel normativo:** Compuesto por procedimientos, guías e instrucciones técnicas. Son documentos operativos que determinan las tareas concretas a realizar en cada proceso. La aprobación de estos niveles es responsabilidad del Comité de Seguridad TIC.

Para asegurar la efectividad de este marco normativo, se establecen las siguientes directrices de gestión:

- El Comité de Seguridad TIC revisará anualmente el cuerpo normativo, proponiendo las mejoras necesarias para adaptarlo a la evolución tecnológica.
- La PSI actúa de forma coordinada y complementaria con la Política de Privacidad de la empresa en materia de protección de datos personales.
- Toda la normativa estará a disposición de los empleados en soporte digital o papel, siendo de especial importancia para el personal que opera o administra los sistemas.
- El contenido de estos documentos formará parte integrante de los planes de formación y concienciación de los usuarios.

16 Terceras partes

Cuando **Q Innovate Consultores** preste servicios a otros organismos o maneje información de terceros, se les hará partícipes de la presente Política de Seguridad de la Información, estableciendo canales formales para el reporte y la coordinación entre los respectivos Comités de Seguridad, así como procedimientos conjuntos de reacción ante incidentes. Del mismo modo, cuando se utilicen servicios de terceros o se ceda información a colaboradores externos, estos serán informados de la presente política y de la normativa de seguridad que afecte a dichos servicios, quedando sujetos a las obligaciones establecidas en la misma y pudiendo desarrollar sus propios procedimientos operativos para satisfacerlas. En todo caso, se garantizará que el personal de estas terceras partes cuente con un nivel de concienciación en materia de seguridad al menos equivalente al exigido internamente en esta organización, estableciendo para ello procedimientos específicos de reporte y resolución de incidencias.

En cumplimiento de lo dispuesto en el Real Decreto 311/2022 (ENS) y sus Instrucciones Técnicas de Seguridad, los operadores del sector privado que provean soluciones o servicios a **Q Innovate Consultores** deberán estar en condiciones de exhibir su correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad para sistemas de categoría BÁSICA, o la Certificación de Conformidad para sistemas de categoría MEDIA o ALTA. No obstante, atendiendo a las especialidades del sector y a la posible dependencia o exclusividad de ciertos proveedores, en caso de que no se disponga de terceros con las conformidades requeridas, se exigirán medidas de seguridad acordes a la valoración del riesgo del servicio. En estos escenarios, el Responsable de Seguridad emitirá un informe técnico precisando los riesgos y su tratamiento, el cual deberá ser aprobado por el Responsable de la Información y el del Servicio, o elevado al Comité de Seguridad para su validación y autorización previa al inicio de la relación contractual.

17 Mejora continua

La gestión de la seguridad de la información en **Q Innovate Consultores** se concibe como un proceso dinámico y en permanente actualización. Dado que los cambios en la organización, la evolución de las amenazas, los avances tecnológicos y las modificaciones legislativas impactan directamente en el nivel de protección, se implanta un proceso de mejora permanente que comportará las siguientes acciones:

- Evaluación periódica de la presente PSI para asegurar su alineación con los objetivos estratégicos.
- Revisión sistemática de los activos y su categorización, siguiendo las directrices de las guías del Centro Criptológico Nacional (CCN).

- Ejecución obligatoria de la evaluación de riesgos con periodicidad mínima anual para detectar nuevas vulnerabilidades.
- Realización de auditorías internas y, cuando proceda por la categoría de los sistemas, auditorías externas para verificar el cumplimiento del ENS.
- Revisión crítica y ajuste de las salvaguardas implantadas para verificar su eficacia real.
- Revisión y actualización constante de las normas, procedimientos e instrucciones técnicas de desarrollo para que respondan a la realidad operativa de la entidad.

18 Desarrollo de la política de seguridad de la información

El cumplimiento de esta PSI se articula mediante normativas y procedimientos técnicos alineados con el ENS, cuya organización y acceso se rigen por una Norma para la Gestión de la Documentación específica. Corresponde al Comité de Seguridad TIC la revisión anual de todo el cuerpo normativo, encargándose de proponer las mejoras necesarias para su aprobación por el órgano que validó el documento original, garantizando así la actualización permanente del sistema.

19 Capacidad de Vigilancia Continua SOC

Como parte esencial de la estrategia de defensa de **Q Innovate Consultores**, se establece la obligatoriedad de mantener una función de vigilancia proactiva, alineada con los requisitos de monitorización del ENS y los estándares internacionales de seguridad:

- Se garantiza la operatividad de un Centro de Operaciones de Seguridad (SOC) con capacidad técnica para la detección temprana de amenazas, la monitorización de eventos anómalos y la supervisión constante de la integridad de los activos críticos.
- Se gestionará los registros de actividad (logs) bajo estrictos controles de seguridad, asegurando que la evidencia técnica sea íntegra, fidedigna y esté disponible tanto para los procesos de mejora continua como para auditorías oficiales o investigaciones forenses.
- La actividad del SOC se integra plenamente en el Sistema de Gestión de la Seguridad de la Información (SGSI). Esta función proporcionará los indicadores

clave (KPIs y métricas) necesarios para que la Dirección y el Comité de Seguridad puedan evaluar el estado real del riesgo y tomar decisiones estratégicas informadas.