1. APROBACIÓN Y ENTRADA EN VIGOR

Texto revisado y aprobado el día 26 de junio de 2020 por el Comité de Seguridad y Servicios. En adelante, nos referiremos al Sistema de Seguridad de la Información del **ENS,** cuándo utilicemos el término **SGSI** (Sistema de Gestión de la Seguridad de la Información) dada su integración en el sistema.

Siguiendo las recomendaciones de la GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402), y en función de nuestro alcance, los comités del Sistema ENS y el de seguridad y servicios se podrán realizar al mismo tiempo dada la integración y equivalencia de los mismos en QUENTAL. De la misma manera el Responsable de Seguridad y Servicios, será también el Responsable de Seguridad ENS.

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

2. INTRODUCCIÓN

Para el cumplimiento de su Misión, la prestación de los Servicios identificados y el cumplimiento de sus objetivos, objeto del alcance, QUENTAL depende de los llamados sistemas TIC (Tecnologías de Información y Comunicaciones). Estos sistemas deben ser administrados con agilidad y diligencia, tomando las medidas de seguridad adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios objeto del alcance, actuando preventivamente, supervisando la actividad diaria y reaccionando con eficacia y eficiencia a los incidentes de seguridad, y garantizando a su vez el cumplimiento de todas las obligaciones legales aplicables, la confidencialidad, integridad y disponibilidad de los sistemas de información. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios objeto del alcance. Esto implica que el área de Sistemas de la organización debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios objeto del alcance, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta eficaz y eficiente a los incidentes de seguridad para garantizar la continuidad de los servicios prestados, objeto del alcance. Los diferentes departamentos deben concienciarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos involucrados deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS, bajo la supervisión y coordinación del Área de Sistemas.

2.1. Prevención de Incidentes

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios, objeto del alcance, se vean perjudicados por incidentes de seguridad. Para ello el área de Sistemas debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el departamento de Sistemas debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Monitorización y detección de Incidentes

Dado que los servicios, objeto del alcance, se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y revisión sobre los recursos, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma ágil, eficaz y eficiente.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

Por su parte, el Reglamento General de Protección de Datos en sus artículos 33 y 34, respectivamente, obliga a notificar las violaciones de seguridad de datos personales a la Agencia Española de Protección de Datos cuando existe riesgo para los interesados y a los propios interesados cuando la violación suponga un alto riesgo para ellos. Por ello se deberán establecer controles internos para identificar y catalogar este tipo de incidencias relacionadas con datos personales y comunicarlas al Responsable de Seguridad.

2.3. Respuesta ante Incidentes

Las áreas o departamentos involucrados deben:

- Responder eficazmente a los incidentes de seguridad, mediante los mecanismos establecidos por el área de Sistemas.
- Designar un único punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Ejecutar los protocolos para el intercambio de información relacionada con el incidente, establecidos por el área de Sistemas. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. Recuperación ante Incidentes

Para garantizar la disponibilidad de los servicios críticos, el departamento de Sistemas debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Todos los servicios de delegación por parte del Cliente, referidos a la Gestión, el Mantenimiento y el Soporte de las Infraestructuras de Tecnologías de la Información, en base a la declaración de aplicabilidad vigente.

4. MISIÓN

QUENTAL es una empresa de servicios y soluciones tecnológicas de capital 100% español con un equipo humano de más de 500 personas que se fundamenta sobre la Calidad, la Innovación, el Talento, la Flexibilidad, que son los valores más importantes para la organización. El Sistema Integrado de Gestión Avanzada de la Calidad tiene como finalidad garantizar la satisfacción de los clientes y conseguir unos servicios competitivos, comprometiéndonos a cumplir con los requisitos derivados de las necesidades de nuestros clientes, con una gestión transparente, eficiente y responsable. Para ello, el Sistema Integrado de Gestión Avanzada tiene como objetivos principales:

1. Gestión y control eficaz de los servicios objeto del alcance.
2. Implementar con eficacia la continuidad del servicio objeto del alcance.
3. Mejorar de forma continua nuestros Sistemas Integrados de Gestión.
4. Cumplimiento de los requisitos legales aplicables y otros requisitos de los clientes.
5. Asegurar la confidencialidad, disponibilidad e integridad de la información.
6. Asegurar una prestación de los servicios, objeto del alcance, realizados a los clientes eficiente y eficaz.

7. Cumplir los requisitos acordados mediante acuerdos de nivel de servicio.
8. Asegurar que todos los servicios implicados garantizan la satisfacción en el cliente.
9. Garantizar un servicio continuado y la gestión adecuada de las incidencias.
10. Gestionar los riesgos eficientemente.
11. Fomentar la comunicación segura, interna y externa.
12. Asignación eficiente de funciones, recursos y responsabilidades.
13. Concienciación, formación y motivación del personal de la Compañía, sobre la importancia del desarrollo e implantación de un Sistema Integrado de Gestión Avanzada de Calidad y sobre su implicación en el cumplimiento de las expectativas de los clientes y la protección de su información.
14. Fidelización de los clientes.
15. Cooperación con clientes y proveedores.
16. Adaptación a la evolución / tecnologías del mercado.

5. MARCO NORMATIVO

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

1. El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
2. Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
3. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
4. La Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales de 13 de diciembre, tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/67 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, garantizando el derecho fundamental de las personas físicas a la protección de datos, amparado por el artículo 18.4 de la Constitución y garantizar los derechos digitales de la ciudadanía, conforme al mandato establecido en el artículo 18.4 de la Constitución.
5. El 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 (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.

6. Ley 39/2015 de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas, tiene por objeto regular los requisitos de validez y eficacia de los actos administrativos, el procedimiento administrativo común a todas las Administraciones Públicas, incluyendo el sancionador y el de reclamación de responsabilidad de las Administraciones Públicas, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria.
7. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, relativo a la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados, de conformidad con el artículo 149.1.21.a de la Constitución.
8. Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal de Delitos Informáticos.
9. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. La presente ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
10. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
11. Ley 59/2003, de 19 de diciembre, de firma electrónica. Tiene como objetivo fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. Además esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comité: Funciones y Responsabilidades

QUENTAL dispone de un Comité de Seguridad y Servicios para la gestión del Sistema y velar por el correcto cumplimiento de las políticas y normas implantadas en la organización. El Comité está compuesto por los siguientes responsables:

Dirección/Área	Representante
Dirección General	Carlos Gómez Lledías

Resp. Calidad, Procesos e Innovación	César Tendero Márquez
Resp. de Seguridad ENS y Servicios	José María López Lombana

El Comité es el encargado de realizar las siguientes funciones dentro del sistema de gestión:

a. Apoyar al Responsable de Seguridad ENS y Servicios para que sus decisiones sean llevadas a cabo con éxito.
b. Coordinar y gestionar todos los servicios y soluciones prestados por la organización, incluidos en el catálogo de servicios y soluciones, para asegurar que se satisfacen todos los requisitos definidos.
c. Decidir, tras las revisiones del sistema, aquellas acciones necesarias para la mejora continua en cuanto a Seguridad.
d. Revisar y Aprobar las Políticas de Seguridad y Servicios de la organización anualmente o cuando se produzcan cambios significativos en la misma. Una vez revisada, será la dirección quien la apruebe.
e. Definir el enfoque que se debe dar a la evaluación y gestión de riesgos para la consecución de los objetivos definidos.
f. Asegurar que los activos se gestionan conforme a los requisitos legales y regulatorios vigentes.
g. Hacer de intermediarios entre el Responsable de Seguridad ENS y Servicios y todas las personas de la organización involucradas en el alcance del sistema.

El Comité, con pleno poder de decisión ejercerá de **dueño de los riesgos** detectados en los análisis de riesgos realizados en **QUENTAL**. Para ello, se asegurará de la correcta realización del análisis de riesgos, el establecimiento del nivel de riesgo aceptable, la aprobación del plan de tratamiento de riesgos y la aceptación de los riesgos residuales (reevaluación de riesgos), todo ello, disponiendo de conocimientos sobre la metodología de análisis de riesgo. El Comité se reunirá, al menos, una vez al año para verificar el correcto funcionamiento de los Sistemas de Gestión implantados en la organización. En caso de que el Comité lo considere oportuno, y debido a circunstancias que así lo requieran, se podrán convocar tantas reuniones extraordinarias como sea necesario. A las reuniones del Comité se podrán invitar a todas aquellas personas que se considere necesario, en función de los temas a tratar.

Para convocar de manera formal una reunión de Comité, el Responsable de Calidad enviará una convocatoria por correo electrónico a todos los componentes del Comité, así como a aquellas personas que se consideren oportunas, indicando el orden del día con todos los puntos a tratar en dicha reunión.

Las conclusiones acordadas en las reuniones del Comité quedan documentadas en un acta, la cual es aprobada o rectificada en el primer punto de la siguiente sesión del Comité, por todos los asistentes a la reunión y guardada como evidencia de la asistencia y registro del funcionamiento del mismo. Las actas se archivan como evidencia documental de las decisiones tomadas por parte del Comité.

Este Comité, puede hacerse al mismo tiempo que el Comité de Calidad General, siempre y cuando, se establezcan los puntos tratados de Servicios y Seguridad.

6.2. Roles: Funciones y Responsabilidades

6.2.1. Responsable del Sistema (ENS)

Está formado por un comité. Los miembros responsables del comité son:

- Director General: Carlos Gómez Lledías.
- Responsable de Seguridad ENS: José María López Lombana.
- Responsable de Calidad, Procesos e Innovación: César Tendero Márquez.

Las **funciones** son las siguientes:

- Establecer los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinar y Aprobar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad (ENS).
- **Determinar la Categoría del Sistema y su Aprobación** dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad (ENS).
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Solicitar opinión al Delegado de Protección de Datos sobre las violaciones de seguridad de datos personales y en su caso, recomendar la notificación a la Agencia Española de Protección de Datos y /o a los propios interesados.
- Tiene la responsabilidad última del uso que se haga de cierta información y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- 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.
- El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección, debe ser acordada por todos los miembros del Comité.

6.2.2. Responsable de Seguridad ENS y Servicios

El responsable de Seguridad y Servicios tiene atribuidas las siguientes **funciones**:

a. Coordinar y mantener el Sistema Integrado de Gestión Avanzada (SIGA) que cubre los aspectos relativos a la seguridad conforme al ENS.

b. Asegurar el cumplimiento de planes y objetivos del Sistema de Gestión.

c. Hacer revisar y hacer mantener, al administrador de sistemas, actualizada la documentación, así como el análisis y evaluación de riesgos, revisando regularmente los resultados para asegurar la continua idoneidad, eficacia y efectividad del mismo, así como de los controles implantados.

d. Garantizar que el Sistema funciona, reaccionando ante cualquier evento y evolucionando hacia la mejora continua, manteniendo informada a la alta Dirección sobre las oportunidades detectadas.

e. Analizar los informes de auditoría y elevar al Comité las conclusiones de este análisis.

f. Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.

Por otro lado, el responsable del sistema tiene atribuidas las siguientes **obligaciones**:

a. Guardará secreto de la información de carácter personal que conozca en el desempeño de su función, aún después de haber abandonado la organización.

b. Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales sea responsable.

c. Conocer la normativa interna en materia de seguridad y calidad. Dicha normativa puede consistir en normas, procedimientos, reglas y estándares, así como posibles guías.

d. Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.

e. No ceder ni comunicar a otros las contraseñas, de carácter personal, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.

f. Velar por el correcto cumplimento de la normativa legal aplicable, especialmente en materia de protección de datos personales y propiedad intelectual.

Perfil: El *Responsable de Seguridad ENS y Servicios,* hará de intermediario entre la organización y los recursos bajo el alcance del sistema. Ha de ocupar un cargo relevante en la organización y conocer bien el funcionamiento de los servicios y departamentos implicados en el sistema, ya que deberá tomar decisiones que pueden afectar al funcionamiento de la misma.

Al ser intermediario con los distintos procesos del sistema debe poseer un perfil de gestión de recursos, tanto técnicos como humanos, para la coordinación de todos los responsables de cada proceso de sistema.

La persona designada para ocupar este cargo debe poseer una experiencia mínima de 3 años.

Persona designada: Persona asignada y aprobada en los Comités de Seguridad y Servicios.

6.2.3. Administrador de Sistemas TIC

El Responsable de sistemas tiene atribuidas las siguientes **funciones**:

a. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

b. Como administrador de todos los accesos a los ficheros y recursos de la instalación pueden tener per se acceso a los mismos.

c. Analizar posibles transgresiones e irregularidades en los accesos.

d. Evaluar la seguridad de paquetes, aplicaciones, productos y dispositivos, antes de su adquisición o implantación.

e. Dar soporte técnico en materia de seguridad, a los desarrolladores, técnicos y usuarios en general.

f. Se encarga de administrar y monitorizar el correcto funcionamiento del sistema

Por otro lado, el Responsable de sistemas tiene atribuidas las siguientes **obligaciones**:

a. Guardará secreto de la información de carácter personal que conozca en el desempeño de su función, aún después de haber abandonado la organización.

b. Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales sea responsable.

c. Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.

d. No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.

e. No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.

f. Proteger las copias de datos que en su caso estuvieran en su poder.

g. No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.

Perfil: La persona designada para ocupar este cargo debe poseer una experiencia mínima de más de 2 años. Debe poseer una formación mínima de FP/Módulo Informático.

Persona designada: Persona asignada y aprobada en los Comités de Seguridad y Servicios. **El Responsable de Sistemas TIC es el Responsable de Seguridad ENS y Servicios en QUENTAL**.

6.2.4. Personal Técnico

El Personal Técnico tiene las siguientes **responsabilidades**:

a. Desarrollo del código efectivo de las aplicaciones que le sean asignadas, basándose en los requerimientos previos del analista, o del arquitecto de software.

b. Realizar una codificación libre de errores, efectuando las pruebas necesarias para tal efecto.

c. Realizar una correcta gestión de versiones en el desarrollo.

d. Mantener el código organizado en repositorios que permitan realizar una correcta trazabilidad sobre todos los cambios que se realizan.

e. Documentar, tanto en el propio código, insertando comentarios que faciliten su compresión, como en la documentación del proyecto, detallando los procesos, algoritmos y funciones empleados en la solución de cada uno de los desarrollos.

f. Realizar su desarrollo aplicando prácticas seguras de codificación desde el punto de vista de la seguridad de la información (Desarrollo Seguro).

g. Informar en todo momento del estado y situación de cada uno de los proyectos en los que está involucrado.

h. Mantener el código actualizado y funcional, en base de los nuevos requerimientos que le sean solicitados.

Perfil: En función del puesto requerido para cubrir las necesidades del servicio (técnico de sistemas, programador, analista programador, analista orgánico, analista funcional, etc.).

6.2.5. Personal

Las **funciones** y **obligaciones** atribuidas al personal de **QUENTAL**, son las siguientes:

a. Acceder únicamente a los datos que necesite para el ejercicio de sus funciones.

b. Todos los datos de carácter personal que con motivo del desempeño de los trabajos que les sean encomendados conozcan los usuarios, son confidenciales y habrán de guardar estricta reserva al respecto, no divulgándolos más allá de lo estrictamente necesario para realizar su trabajo.

c. Cualquier incidencia acaecida habrá de ser comunicada de acuerdo con lo indicado en el Procedimiento de Gestión de incidencias y peticiones de servicio.

d. El deber de no sacar fuera del ámbito de QUENTAL ninguna clase de datos sin autorización expresa del Responsable del SGS y SGSI.
e. El deber de no dejar su pantalla de acceso a los Sistemas e información activa cuando por cualquier causa deje su puesto de trabajo desatendido.
f. La obligación de disponer de clave de acceso a los ordenadores y modificarla cuando así se establezca.
g. El cumplimiento estricto de las normas, políticas y procedimientos de seguridad contenidos en este Documento de Seguridad que les afecten.
h. Queda expresamente prohibido destruir, alterar o dañar de cualquier otra forma los datos, programas o documentos electrónicos.
i. Queda expresamente prohibido intentar borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
j. Ejecución de los servicios del alcance.

6.3. Procedimiento de Designación

El Responsable del Sistema como el Responsable de Seguridad de la Información ENS, serán nombrados por el Comité de Seguridad y Servicios. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.4. Política de Seguridad de la Información

Será misión del Comité de Seguridad y Servicios la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Comité de Seguridad y Servicios y difundida para que la conozcan todas las partes involucradas.

7. DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios objeto del alcance, deben ser tratados datos de carácter personal. QUENTAL dispone de un análisis de riesgos de seguridad con controles y medidas que mitigan o eliminan los riesgos detectados para determinados tratamientos de riesgos altos, para lo que se ha elaborado una Evaluación de Impacto en la protección de los datos, que, entre otros aspectos, identifica los riesgos en materia de seguridad y recoge medidas y controles para que el riesgo residual sea aceptable.

8. DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Aunque la organización no cumple con la obligatoriedad de designar un DPD, tanto la RGPD, como las Recomendaciones del Grupo 29, como la LOPDGDD 3/2018, establecen como buena práctica y motivo de

atenuante en caso de infracción, haber designado un DPD, de manera que QUENTAL ha tomado la decisión de hacerlo.

El Delegado de Protección de Datos será único para toda la organización, informándose de su nombramiento y cese a la Agencia Española de Protección de Datos. Las funciones del Delegado de Protección de datos serán las indicadas en el ya mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia.

Se identifican las siguientes funciones y obligaciones de la figura del DPD, extraídas tanto del RGPD, como de la LOPD (LOPDGDD 3/2018), así como de las Recomendaciones del Grupo 29:

- Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
- Supervisar el cumplimiento de la normativa
- Asesorar respecto de la evaluación de impacto relativa a la protección de datos, para lo que deberá aconsejar al RT sobre:
    - si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
    - qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
    - si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
    - qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados.
    - si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con la normativa general de protección de datos.
- Cooperar con la autoridad de control
- Actuar como punto de contacto para cuestiones relativas al tratamiento
- Ayudar al responsable o el encargado del tratamiento a controlar el cumplimiento interno del RGPD, para lo que necesitará:
    - recabar información para determinar las actividades de tratamiento,
    - analizar y comprobar la conformidad de las actividades de tratamiento, e
    - informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Deberá considerar debidamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.
- Elaborar inventarios y mantener un registro de las operaciones de tratamiento basados en la información que les proporcionan los diversos departamentos de su organización responsables del tratamiento de datos personales.
- Comunicar a los órganos de administración y dirección del RT o del ET la existencia de una vulneración relevante en materia de protección de datos, y proporcionar las medidas necesarias para evitar la persistencia de esta conducta.
- Recibir las reclamaciones contra un RT o ET presentadas por un afectado, comunicar al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

- Recibir las reclamaciones contrato un RT o ET por parte de un afectado, directamente de Agencia Española de Protección de Datos o, de las autoridades autonómicas de protección de datos, cuando el afectado se ha dirigido a las autoridades de control directamente, debiendo dar respuesta en el plazo de un mes.

Está formado por un Comité formado por los siguientes miembros de la organización:

- Dirección General: Carlos Gómez Lledías.
- Responsable de RRHH: Carolina González Arrache.
- Responsable de Seguridad de la Información: José María López Lombana.
- Responsable de Calidad, Procesos e Innovación: César Tendero Márquez.

9. GESTIÓN DE RIESGOS

Los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Comité de Seguridad y Servicios, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

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

Una vez realizado el análisis de riesgos de los activos, objeto del alcance, el comité de seguridad debe aprobar los resultados obtenidos.

A continuación, el comité debe aprobar los niveles de riesgo asumibles por la organización. Para aquellos activos que no se asuman riesgos asociados, se debe establecer un plan de tratamiento de riesgos que incluya la definición de controles a implementar, plazos, responsabilidades y descripción de las actividades a realizar.

El plan de tratamiento de riesgos contendrá, además de la información descrita anteriormente, el seguimiento de las actividades de manera que su visualización permita el estado actual de cada uno de los controles.

Aparte de la aplicación de controles, existe la posibilidad de transferir los riesgos o asumirlos:

- Los riesgos se pueden transferir a través de acuerdos con compañías de seguros o proveedores.
- En cuanto a la posibilidad de asumir riesgos, esta acción debe ser realizada con el consentimiento escrito de la Dirección.

Sin embargo, en cualquiera de los casos anteriores, el dueño del riesgo será el Responsable del Comité de Seguridad y Servicios.

Con el fin de asegurar el buen funcionamiento del proceso de gestión de riesgos, es necesario realizar un seguimiento periódico de la ejecución del plan de tratamiento de riesgos que permita conocer el estado de cada uno de los controles, asegurando el compromiso con la mejora continua del sistema de gestión, así como realizando la verificación, de que se han proporcionado los recursos necesarios para la implementación de los controles, y por tanto, el adecuado tratamiento, de al menos, los riesgos no asumibles por la organización.

Una vez implementados los controles, al menos una vez al año, se llevará a cabo la reevaluación de riesgos, donde se analizará el grado de eficacia y desempeño de los controles implementados, y cómo estos, han influenciado en las variables que intervienen en el cálculo del riesgo.

Como parte de la reevaluación de riesgos, se deberán tener en cuenta también todos aquellos cambios, incidentes y cualquier otro tipo de evento, que pudieran haber conllevado modificaciones en las variables que intervienen en el cálculo del riesgo, así como cualquier otra previsión a futuro, de qué situaciones pueden afectar a la seguridad de la información de la organización.

Una vez finalizada la reevaluación de riesgos, se aportarán unos resultados, en la Revisión por la Dirección, donde se revisarán los riesgos residuales, que en caso de existir, deberán ser aprobados por el Responsable del Proceso, conjuntamente con el Responsable del propio riesgo.

Los resultados de la reevaluación, servirán como información de entrada para la toma de decisiones, para entre otros apartados, plantear los objetivos de seguridad, definir cambios en el nivel de riesgo aceptable o asumible, o para determinar la estrategia de seguridad de la información a seguir, por parte de la organización.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

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

- Política de Seguridad de la Información y Gestión de Servicios TI, conforme a las normas ISO 27001- ISO 20000.
- Política de Gestión de la Calidad, conforme a la norma ISO 9001.
- Política de Gestión Medioambiental, conforme a la norma ISO 14001.
- Política Anticorrupción y Antisoborno.

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

La normativa de seguridad estará disponible en la Web Corporativa y en el SIGA (Drive de Calidad) accesible para personal externo e interno.

11. OBLIGACIONES DEL PERSONAL

Todos el personal involucrado en el alcance del sistema de la seguridad de la información de QUENTAL, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad y Servicios disponer los medios necesarios para que la información llegue a los afectados.

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados involucrados en el alcance del sistema al menos cada dos años, y en particular a los de nueva incorporación, así como a la difusión entre los mismos de la Política de seguridad y de su desarrollo normativo.

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.

12. TERCERAS PARTES

Cuando QUENTAL preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. Cuando QUENTAL utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Firma de Aprobación:

El Comité de Seguridad y Servicios de QUENTAL

(Aprobado el 26/06/2020)

Fdo.: José María López Lombana

Responsable de Seguridad y Servicios