SGSI-REG-MA-01

Política de Seguridad de la Información

Realizado:	Responsable Seguridad	Fecha:	Diciembre 2023
Revisado:	Comité Seguridad	Fecha:	Enero 2024
Aprobado:	Dirección General	Fecha:	Junio 2024

CONTROL DE MODIFICACIONES Y REVISIONES:

Versión	Fecha	Apartado modificado/revisado	Descripción modificación/revisión
0.1	12 /2023	Todos	Creación del documento
0.1	01/2024	Angel Lacalle	Revisión y cumplimentación
1.0	04/2024	Juan Antonio Menéndez	Revisión y aprobación
1.1	06/2024	Juan Antonio Menéndez	Correcciones menores
1.2	06/2025	Juan Antonio Menéndez	Correcciones menores

Contenidos

1. Introducción

Quantyca Software Solutions, S.L. (en adelante, Quantyca) es una compañía tecnológica de capital español nacida en el 2007. Quantyca es fabricante y propietaria de la plataforma UBYQUO y todos sus módulos-software para la automatización de detalle de procesos operativos y de negocio y lideran el mercado de la mediana y pequeña empresa transformando procesos y tareas repetitivas y manuales, en procesos automáticos y desatendidos. Su filosofía es implantar la tecnología más avanzada para reducir tiempos, ahorrar costes y trasladarlo en valor hacia sus clientes. Se han especializado en tecnologías de captura de datos y gestión de documentos y su contenido, independiente de la complejidad de la extracción y del destino final de esos datos.

Esta política es entendida, implantada y mantenida al día en todos los niveles de la empresa y cuenta con el total compromiso y apoyo de la Dirección de Quantyca, quien la establece, desarrolla y aplica por medio de su Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) según la norma UNE-ISO/IEC 27001.

2. Alcance

Esta Política se aplica dentro del alcance de gestión integrado, siendo de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios dentro del mismo.

3. Contenido

La calidad y la seguridad de los servicios son objetivos estratégicos para Quantyca y la información relacionada con ellos constituye un activo fundamental para la toma de decisiones eficientes. Por estas razones la Dirección declara su compromiso expreso con la mejora continua de su Sistema de Gestión de Seguridad de la Información como pilar de una estrategia orientada a la gestión de los riesgos y la consolidación de una cultura basada en la seguridad.

El alcance del Sistema de Gestión es el siguiente:

"*Los sistemas de información que dan soporte a las Soluciones de Automatización de Documentos y Datos de la plataforma UBYQUO, incluyendo expresamente un Sistema de Facturación y una Solución Privada de gestión de Facturas Electrónicas en compliance con las Leyes 11/2021 (Ley Antifraude) y 18/2022 (Ley Crea & Crece), conforme a la declaración de aplicabilidad vigente".*

Términos y definiciones

- **SGSI**: Son las siglas del Sistema de Gestión de la Seguridad de la Información (regulado por la Norma UNE-ISO/IEC 27001) que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Parte interesada**: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
- **Autenticidad**: Propiedad de que una persona y o empresa que ha accedido y utilizado la información es lo que afirma ser.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
- **Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona y o empresa.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Tratamiento de riesgos**: Proceso de modificar el riesgo, mediante la implementación de controles.
- **Datos personales**: Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.

Misión y marco legal y regulatorio

Con la implantación de un SGSI bajo la Norma UNE ISO/IEC 27001 se fortalece la seguridad de nuestros servicios, así como de la información y datos que incluyen y que son necesarios para su correcta y adecuada prestación.

Quantyca trata documentos y datos empresariales (facturas, extractos bancarios, nóminas...), dentro de los que es posible contengan determinados datos de carácter empresarial (razón social, dirección empresarial, cifs...) que deberán registrarse y mantenerse actualizados mediante los documentos "Registro de Actividades de Tratamiento" y "*Mapa de riesgos y oportunidades*" con el objeto de facilitar el control, la gestión y la protección de los derechos, analizando los riesgos y aplicando medidas de seguridad específicas para cumplir con 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 (Reglamento General de Protección de Datos), equivalente a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que se creó para facilitar la aplicación y cumplimiento en España.

El SGSI de Quantyca se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, así como el resto de las normativas aplicables recogidas en el documento "*Marco Normativo*".

Liderazgo y compromiso de la dirección

La dirección de Quantyca se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la entidad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad de la Información que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de Quantyca de fomento de la sociedad de la información en España.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI en los servicios y procesos de la entidad.
- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI.
- Asegurar que el SGSI consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la dirección, liderando a sus áreas de responsabilidad en seguridad de la información. El detalle de las funciones específicas del Comité de Seguridad de la Información, se describen en su acta de constitución.

Objetivos de 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:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.

- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- 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.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Los recursos necesarios
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

Establecimiento, implantación, mantenimiento y mejora del SGSI de Quantyca y directrices para la gestión de la documentación

El despliegue del SGSI de Quantyca se realiza a partir del "*Mapa de riesgos y oportunidades*" que permite determinar el nivel de seguridad requerido por la organización e identificar los controles necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, conforme al Anexo A de la norma ISO 27001.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente y estar disponibles como información documentada que deberá ser revisada y aprobada por el Comité de Seguridad de la Información en representación de la Dirección General.

La presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos e incluirse en la documentación del sistema:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo) que tendrá la obligación de aplicarla en la realización de sus actividades laborales.

La información documentada será clasificada en: Pública, Interna y Confidencial dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en el "*Procedimiento de Clasificación y Etiquetado de la Información*".

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI de Quantyca con los requisitos de la Norma ISO/IEC 27001 para el SGSI, por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

Funciones y responsabilidades de seguridad de la información

El Comité de Seguridad de la Información procederá a revisar y a proponer la aprobación de la presente Política de Seguridad de la Información a la Dirección General de Quantyca que será el **Responsable de la Información**.

Además, el Comité de Seguridad de la Información centralizará los mecanismos de coordinación y resolución de conflictos entre los responsables que se indican a continuación, que se tratarán mediante debate durante las reuniones de los miembros de dicho comité y que serán moderados por la Dirección General:

- El **Comité de Seguridad**, en representación de la Dirección General de Quantyca, será el órgano encargado de aprobar la política y será la responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI/ENS de la entidad.
- El **Responsable de Seguridad de la Información** será el encargado de notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI/ENS de la entidad (incluyendo la firma de la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables derivadas del Análisis de Riesgos), y de sus auditorías, con el **Responsable de Sistemas** que se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información, y con el **Responsable del Servicio**, cuya figura recae en los directores de las áreas de la entidad, que se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios.
- El Responsable de cada información y/o del servicio afectado por el análisis y gestión de riesgos se indicará en el "*Mapa de riesgos y oportunidades*" de Quantyca que recogerá los criterios que determinarán el nivel de seguridad requerido.
- El **Responsable de Protección de Datos** será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos cumplimiento del Reglamento UE 2016/679 General de Protección de Datos (RGPD) y de la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y de garantía de derechos digitales (LOPDGDD), por lo que trabajará en coordinación con el Responsable de Seguridad de la Información y con el Responsable de Sistemas.
- Todo el **personal de la organización**, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del SGSI de Quantyca en sus actividades laborales que afecta a su desempeño en seguridad de la información.

Revisión de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será examinada en las revisiones del sistema por la Dirección a través del Comité de Seguridad de la Información, siempre que se produzcan cambios significativos y como mínimo una vez al año.

Aprobación, difusión y aplicación de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será aprobada por la Dirección General de Quantyca mediante firma y difundida a las partes interesadas.

Así mismo, la Dirección General de Quantyca dotará de los recursos necesarios para la aplicación efectiva de esta política y para su buen desarrollo tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el SGSI de la entidad.

En Las Rozas, a 18 abril de 2024