QUALITY & KNOWLEDGE

MORE THAN YOUR IT SERVICE PARTNER

ISO 27001:2022

Política de Seguridad

Versión 1.0 – Liberado el 20 de mayo de 2024

Roberto López Rodríguez

Responsable SGSI

Histórico de revisiones

Rev.	Fecha	Autor	Descripción
1	20/05/2024	Roberto López R.	Documento Original

Indice

Introducción.

Este documento constituye la **Política de Seguridad de la Información** de Quality & Knowledge On IT Services, dicha política recoge nuestra postura en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad de nuestra organización en cuanto a la seguridad.

El objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Quality & Knowledge On IT Services, es una empresa de servicios de desarrollo de software y atracción y talento, ubicada en Av. Ejército Nacional Mexicano 373-piso 5, Chapultepec Morales, Granada, Miguel Hidalgo, 11520 Ciudad de México, CDMX.

Política General de Seguridad.

Quality & Knowledge On IT Services utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios, por lo que es consciente de que estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.

Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a Internet (ciberataques).

La política de Quality & Knowledge On IT Services es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias. Para este fin hemos decidido implantar un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2022 con el objetivo de preservar la **Confidencialidad, Integridad** y **Disponibilidad** de la información, proteger a ésta de un amplio grupo de amenazas y destinado a asegurar la continuidad de nuestros servicios, optimizar los recursos, las oportunidades y la mejora continua.

La dirección de Quality & Knowledge On IT Services, mediante la elaboración e implantación del presente Sistema de Gestión de Seguridad de la información adquiere los siguientes compromisos:

- Desarrollar productos y servicios conformes con los requisitos legislativos, identificando para ellos las legislaciones de aplicación a los diferentes servicios

desarrollados por la organización e incluidas en el alcance al Sistema de Gestión de la seguridad de la información.

- Estableciendo y cumpliendo los requisitos contractuales con las partes interesadas.
- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento con organizaciones especializadas.
- Gestión de la continuidad de los servicios, desarrollando planes de continuidad conforme a metodologías de reconocido prestigio internacional.
- Establecimiento de las consecuencias de la violación de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas
- Actuar en todo momento dentro de la más estricta ética profesional.

Esta política proporciona el marco de referencia para la mejora continua del sistema de gestión de seguridad de la información así como para establecer y revisar los objetivos del sistema de gestión de seguridad de la información, siendo comunicada a toda la organización y siendo revisada anualmente para su adecuación y extraordinariamente cuando concurran situaciones especiales y/o cambios sustanciales en el Sistema de Gestión de Seguridad de la información, estando a disposición público en general.

Alcance.

Esta Política de Seguridad de la Información es de aplicación a todos los servicios prestados por Quality & Knowledge On IT Services que se apoyen en las Tecnologías de la Información y las Comunicaciones, así como a todo el personal, sin excepciones.

Desarrollo de la Política de Seguridad de la Información.

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad de la Información se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por Quality & Knowledge On IT Services.

Conceptos Básicos.

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. (ISO/IEC 27001).

Activo de Información: es todo recurso por medio del cual se almacena, procesa, transmite, divulga, comunica, intercambia, presenta y genera la información, de igual manera la información en sí misma es un activo de información solo que esta se vale de algún medio o recurso para su gestión.

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Roles Involucrados y Responsabilidades.

Director General

Proporcionar y propiciar el liderazgo y los recursos necesarios para implementar y mantener un Sistema de Gestión de Seguridad de la Información (**SGSI**) eficaz.

Comprometerse expresamente con la mejora continua realizando revisiones de la eficacia de los controles implementados y desarrollando medidas para apoyar este proceso.

Responsable de Seguridad de la Información

Es el líder del Equipo de Trabajo de Tecnología de la Información quien a su vez se apoya en expertos técnicos para la implementación, implantación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este rol tiene las siguientes responsabilidades:

- ✓ Velar por la implementación, puesta en marcha y mantenimiento del Sistema de Gestión de Seguridad de la Información.
- ✓ Velar por la revisión de la estructura (políticas, procedimientos, instructivos, roles, responsables y responsabilidades) del Sistema de Gestión de Seguridad de la Información.
- ✓ Hacer seguimiento al plan de trabajo que permita el logro de los objetivos específicos de seguridad de la información de Quality & Knowledge On IT Services.
- ✓ Presentar los cambios, proyectos e iniciativas del SGSI al representante por la Dirección del Sistema de Gestión de Seguridad de la Información.
- ✓ Monitorear y velar por el cumplimiento del Plan Operativo de Seguridad de la Información de Quality & Knowledge On IT Services.
- ✓ Presentar las necesidades de recursos financieros para el desarrollo de proyectos que fortalezcan la gestión de la seguridad de la información con el fin de lograr los objetivos misionales y estratégicos de Quality & Knowledge On IT Services.
- ✓ Obtener la aprobación de la política por parte de la **Dirección General**

Líder Técnico de Seguridad de la Información o también designado como **Oficial de Seguridad de la Información** es aquel profesional o contratista quien implementa y mantiene operativamente el Sistema de Gestión de Seguridad de la Información.

En sus responsabilidades están:

- ✓ Supervisar y coordinar todas las actividades relacionadas con la seguridad de la información que garanticen que la información propiedad de Quality & Knowledge On IT Services y de sus clientes está protegida del acceso y tratamiento no autorizado
- ✓ Proporcionar los recursos humanos, materiales y tecnológicos suficientes para garantizar la adecuada protección de la información

- ✓ Implementar la presente política en sus áreas de Infraestructura y Administración de la Configuración, así como el Sistema de Gestión de Seguridad de la Información (SGSI) definido conjuntamente con el Responsable de Seguridad de la Información

Administrador de Recursos Humanos

Definir la Estrategia de implementación del Sistema de Gestión de Seguridad de la Información (**SGSI**), así como los planes de Capacitación y de Comunicación, tanto los correspondientes a la implementación como los correspondientes al mantenimiento permanente del **SGSI** completo.

Recolectar, consolidar y analizar los Indicadores definidos para evaluar la efectividad de la implementación.

Establecer la estrategia necesaria en caso de desviaciones detectadas durante el análisis de los Indicadores.

Infraestructura/TI

El área de Infraestructura/TI tiene como responsabilidad principal garantizar la operación segura de los sistemas, redes y dispositivos de la organización, en alineación con los requisitos de ISO 27001. Entre sus funciones se encuentra la gestión de accesos y cuentas de usuario, administrando altas, bajas y modificaciones, aplicando el principio de privilegios mínimos e implementando mecanismos de autenticación robusta, como contraseñas seguras y multifactor.

Asimismo, debe asegurar la gestión de redes y comunicaciones, mediante la configuración segura de firewalls, routers y switches, la segmentación de redes y la protección de conexiones remotas a través de tecnologías como VPN o TLS. Esta labor se complementa con la gestión de servidores, sistemas y dispositivos, lo que implica aplicar parches y actualizaciones, realizar configuraciones seguras (hardening) y administrar servicios en la nube de acuerdo con las políticas de seguridad definidas.

Otra responsabilidad esencial es la ejecución y verificación de respaldos, siguiendo las políticas de copias de seguridad, así como la participación en pruebas periódicas de planes de recuperación y continuidad de negocio (DRP). En paralelo, se deben implementar medidas de protección contra malware y amenazas, manteniendo actualizadas las soluciones de seguridad como antivirus o MDR, y monitoreando la red en busca de comportamientos anómalos.

El área también participa activamente en la gestión de incidentes de seguridad, detectando, registrando y escalando los casos que se presenten, en coordinación con el equipo de seguridad. Para ello, mantiene un monitoreo constante y registros de actividad, gestionando bitácoras de accesos, configurando alertas en sistemas críticos y revisando periódicamente los logs.

En cuanto a la infraestructura física y virtual, es responsable de asegurar la protección y el control de acceso físico a equipos. Además, debe brindar soporte a auditorías internas y externas, aportando evidencias técnicas y garantizando el cumplimiento de requisitos regulatorios o contractuales.

Finalmente, el área de Infraestructura/TI debe fomentar la concienciación y apoyo al personal, proporcionando soporte en el uso seguro de los sistemas y participando en capacitaciones, talleres o simulacros relacionados con la seguridad de la información.

Responsables de las áreas de nivel 2.

Facilitar la implementación del Sistema de Gestión de Seguridad en la Información (**SGSI**) en sus respectivas áreas.

Asegurar el cumplimiento de la Política y del SGSI completo, por parte del personal a su cargo.

Apoyar a las áreas correspondientes en la recolección de los indicadores definidos para asegurar el cumplimiento de la Política y del SGSI.

Personal de Quality & Knowledge.

Todo el personal a todos los niveles deberá apegarse a las políticas y procedimientos de seguridad de la informacion establecidos en Quality & Knowledge On IT Services, así como respetar y mantener la confidencialidad de la información, procesos, estándares y demás activos del Sistema de Gestión de Seguridad de la Información (SGSI).

Políticas Generales.

Apego a normatividad

Mantener registro de cumplimiento con las obligaciones legales, regulatorias y contractuales establecidas aplicables relacionadas con la seguridad de la información.

Realizar auditorías internas y externas periódicas.

Acceso a la información, sistemas y recursos de red

Limitar el acceso a la información a aquellos empleados que necesiten acceder a ella para llevar a cabo sus funciones.

Establecer controles de acceso apropiados, como contraseñas seguras y autenticación de dos factores.

Gestión de Riesgos

Evaluar periódicamente a nivel Organizacional los riesgos para identificar y tratar los posibles riesgos de seguridad de la información.

El análisis se realizará:

- ✓ regularmente, una vez al año.
- ✓ cuando haya cambios significativos en la información manejada.
- ✓ cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- ✓ cuando ocurra un incidente de seguridad grave.
- ✓ cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas

Proceso

1. Implementar controles adecuados para mitigar los riesgos identificados.
2. Re evaluar los riesgos una vez implementados los controles.
3. Dar seguimiento a los riesgos hasta su minimizarlos.

Protección de los activos de informacion.

Proteger los activos de información de la organización contra accesos no autorizados, daños, pérdidas o alteraciones.

Implementar medidas de seguridad físicas y lógicas como firewalls, antivirus y copias de seguridad regulares.

Concientización y formación

Proporcionar capacitación y concientización periódicamente a todos los empleados sobre las políticas y procedimientos de seguridad de la información. Se deberá incluir la

identificación de amenazas comunes, buenas prácticas de seguridad y proceso de comunicación de incidentes de seguridad.

Mejora continua

Mejorar continuamente el Sistema de Gestión de Seguridad de la Información (**SGSI**), a través de la revisión regular de su efectividad, la identificación de áreas de mejora y la implementación de acciones correctivas y preventivas.

Establecer, recolectar y analizar indicadores de medición de la efectividad del **SGSI** y generar las estrategias necesarias a fin de mejoras el rendimiento del **SGSI**.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a Seguridad y Privacidad de la Información se refiere.