Propuesta de una Implementación de una Consultoría en la Gestión de la Seguridad de la Información (SGSI) Basados en la Norma ISO/IEC 27001:2022 para obtener la Certificación en la empresa SQA S.A.

Andrés Felipe Forero Gutiérrez, Leidy León Rodríguez, Víctor Manuel Romero Albarracín, Jairo Andrés Zabala Serrano

Especialización En Seguridad Informática,

Fundación Universitaria Compensar

Proyecto fin de grado

Miguel Ricardo Pérez Pereira

22 de noviembre de 2023

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Propuesta de una Implementación de una Consultoría en la Gestión de la Seguridad de la Información (SGSI) Basados en la Norma ISO/IEC 27001:2022 para obtener la Certificación en la empresa SQA S.A.

Andrés Felipe Forero Gutiérrez, Leidy León Rodríguez, Víctor Manuel Romero Albarracín, Jairo Andrés Zabala Serrano

Trabajo de grado presentado como requisito parcial para optar al título de:
Especialización en Seguridad Informática

Director (a):

Título (Ph.D., M.Sc., M.Eng, Ingeniero(a), etc.) y nombre del director(a)

Codirector (a):

Línea de Investigación:

Nombrar la línea de investigación en la que se enmarca el trabajo de investigación

Grupo de Investigación:

Nombrar el grupo en caso que sea posible

Fundación Universitaria Unipanamericana – Compensar
Facultad de Ingeniería, Ingeniería de Especialización en Seguridad Informática
Bogotá, Colombia
2023

Resumen

En la presente era digital, la seguridad va mucho más allá de tan sólo salvaguardar lugares, elementos físicos, o hasta seres vivientes, ya que, aspectos tales como la información de datos económicos, personales y/o empresariales, desempeñan una importancia total, lo que hace que la seguridad sea orientada a proteger dicha información. Para la gran mayoría de empresas, sus activos más preciados giran en torno a la información, y el hecho de que dicha empresa se mantenga actualizada en ámbitos legales, de norma, y en general de políticas se seguridad, resulta vital para eliminar las posibles amenazas informáticas las cuales puedan facilitar el acceso no autorizado, y en general aumentar la vulnerabilidad a su propia seguridad.

La empresa multinacional SQA S. A, posee sedes en México, y en Colombia, varias de sus sedes están ubicadas en Medellín y Bogotá. Actualmente realiza pruebas de calidad del software en sistemas digitales y aplicacionales, pero desde el año 2013, ésta empresa se encuentra laborando con normas ISO, totalmente desactualizadas, lo que la hace mucho más vulnerable a los ciberataques actuales. Lo que se plantea en ésta propuesta, es la implementación de una consultoría en la gestión de la seguridad de la información (SGSI), la cual permita detectar las posibles falencias en las políticas y controles de seguridad de la información que se han de realizar en dicha empresa, y, fundamentada en la norma actual ISO/IEC 27001 de 2022, poder lograr su certificación, lo que le incrementará su nivel de acreditación, en relación a su gestión de seguridad.

Palabras clave:

Consultar, Normativas, Actualizar, Proteger, Información, Seguridad, Ciberataque.

Abstract

In the present digital age, security goes far beyond just safeguarding places, physical elements, or even living beings, since aspects such as economic, personal and/or business data information play total importance, which makes security oriented to protect said information. For the vast majority of companies, their most precious assets revolve around information, and the fact that said company stays updated in legal areas, regulations, and security policies in general, is vital to eliminate possible threats. Computer networks which can facilitate unauthorized access, and in general increase vulnerability to your own security.

The multinational company SQA S. A. has offices in Mexico, and in Colombia, several of its offices are located in Medellin and Bogotá. It currently carries out software quality tests in digital and application systems, but since 2013, this company has been working with completely outdated ISO standards, which makes it much more vulnerable to current cyberattacks. What is proposed in this proposal is the implementation of a consultancy in information security management (ISMS), which allows detecting possible shortcomings in the information security policies and controls that must be carried out in said company, and, based on the current ISO/IEC 27001 of 2022 standard, be able to achieve its certification, which will increase its level of accreditation, in relation to its security management.

Keywords:

Consult, Regulations, Update; Project; informatión, Security, Cyberattack.

Contenido

PÁG.

RESUMEN ..... **V**

INTRODUCCIÓN **1**

ANTECEDENTES Y JUSTIFICACIÓN 1
FORMULACIÓN DEL PROBLEMA 3
OBJETIVO GENERAL 3
Objetivos Específicos *3*
ALCANCES 4
LIMITACIONES 4

1. MARCO TEÓRICO **5**

1.1 SISTEMA DE INFORMACIÓN 5
1.2 SISTEMAS EN GESTIÓN DE SEGURIDAD INFORMÁTICA SGSI: 5
1.3 ¿POR QUÉ IMPLEMENTAR UN SGSI? 5
1.4 NORMA ISO 27001 6
1.5 BENEFICIOS DE LA ISO 27001 DE 2022 6

2. DISEÑO METODOLÓGICO **7**

2.1 DESARROLLO OBJETIVO 1. 7
2.2 DESARROLLO OBJETIVO 2. 7
2.3 DESARROLLO OBJETIVO 3. 7

3. RESULTADOS **8**

4. CONCLUSIONES Y RECOMENDACIONES **9**

4.1 CONCLUSIONES 9
4.2 RECOMENDACIONES 9

BIBLIOGRAFÍA **11**

Introducción

En la actualidad la empresa SQA S.A, es una compañía con más de 19 años de experiencia en la seguridad y el control sobre la calidad del software, y se encarga de proporcionar a las diferentes empresas de seguridad bancaria servicios de aseguramiento de calidad de software adaptados a las necesidades de sus clientes, por medio de enfoque técnico y dinámico y un modelo de trabajo flexible.

Debido a la gran necesidad de confidencialidad en la información de sus clientes, la empresa SQA S.A debe contar con políticas y controles de seguridad acordes con los estándares internacionales, para así evitar incidentes de ciberseguridad que puedan perjudicar a sus clientes. Es importante recalcar que, por ser los clientes de la empresa del sector bancario, manejan información altamente sensible y delicada, por tal motivo es imprescindible un método que minimice o evite tales incidentes.

Teniendo en cuenta los altos índices actuales en "ciberinseguridad", se hace necesario que la empresa cuente con un procedimiento que identifique las falencias en su estructura de administración en preservación de información (SGSI) actual, asegurando así, discreción y acceso total a los bienes preciados, como lo es la información. Disminuyendo así las fugas y/o fallas en ciberseguridad; este procedimiento debe facilitar la certificación de la empresa bajo el estatuto ISO:27001 de 2022, el cual es de carácter internacional describiendo una forma correcta en gestionar y salvaguardar su seguridad, para así evitar o minimizar los incidentes de ciberseguridad que puedan perjudicar el inadecuado uso de la información.

Antecedentes y Justificación

La propuesta para que la empresa SQA S.A logre la certificación ISO 27001 de 2022 se justifica en favor del actual aumento en importancia, sobre seguridad en la información. Esta empresa cuenta con casi dos décadas de conocimiento y experiencia, en el aseguramiento y control sobre la calidad del software, y sus clientes, especialmente del sector bancario, maneja información altamente sensible. La adecuación de políticas y controles de seguridad de alto nivel se ha vuelto una necesidad debido al incremento de amenazas informáticas y al elevado costo que pueda afrontar por los incidentes de seguridad.

El hecho del aumento de acciones invasivas a la privacidad, respeto y acceso a los datos y/o información (triada de la seguridad informática) podría tener consecuencias graves, incluyendo la disminución del nivel de confianza en los usuarios, y a largo plazo, sanciones administrativas.

Al ejercer consultoría sobre los "controles de seguridad en la información, dicha acción actúa como una medida preventiva para que la información posea los niveles de protección idóneos; por esta razón resulta importante efectuar un análisis al sistema de gestión que contiene la empresa SQA S.A., para así, lograr disminuir los riesgos lógicos y físicos contenidos en la información, la cual se envía, analiza, almacena y se distribuye a través del conjunto de procesamiento, considerado como "sistema".

Con la reglamentación ISO 27001 de 2022 se puede mitigar riesgos tecnológicos y vulnerabilidades informáticas si se implementa los controles y adicionalmente los estatutos en seguridad sobre la información de la empresa SQA S. A. Esta Norma ha demostrado su gran potencial para la minimización de los riesgos asociados a ataques informáticos en los entornos empresariales, como se muestra en los casos de éxito en las compañía Tata Consultancy Services (TCS) y Fredrickson international, la cual al haber implementado la norma posee desde ese momento una mayor robustez de seguridad informática para la organización (bsigroup, 2023)

En el año 2018 un grupo de estudiantes de la universidad distrital Francisco José De Caldas se dispuso a la tarea de la elaboración de una propuesta para la implementación de un SGSI para la empresa LOVATO CITY GAS S.A.S basado en la norma ISO/IEC 27001:2013 donde se obtuvieron resultados notables en la asignación de roles, responsabilidades y la importancia de que la empresa cuente con el conocimiento de los riesgos a los que están expuestos tanto a nivel interno como a nivel externo. En una primera fase o estado, la evaluación de los dominios y controles de seguridad según la norma ISO 27001:2013; a partir de este diagnóstico realizaron la presentación de los hallazgos, así como la separación de criticidad de riesgos entre no aceptables y por ejemplo riesgos críticos que recomendaron ser atendidos según lo establece la norma en el menor tiempo posible. En la última fase recomendaron el entrenamiento o concientización de las políticas existentes, las políticas que fueron actualizadas y las 15 nuevas políticas que se establecieron para la empresa, esta capacitación permitiría a los colaboradores estar en la capacidad de saber cómo reaccionar ante un posible ataque y el canal correspondiente para su reporte y/o escalamiento al área pertinente lo que en otras palabras señalaría el correcto funcionamiento en práctica del SGSI para la empresa. (GERALDINE ORTIZ, 2018)

Formulación del Problema

SQA S.A., es una industria de carácter privado, con casi dos décadas de conocimiento y formación en aseguramiento y control de calidad del software. Esta empresa colombiana, fue fundada el 08 de enero de 2004; creada por escritura pública No. 16 y registrada en la ciudad de Medellín. Actualmente la empresa se encarga de garantizar la calidad del software, usando diversas soluciones especializadas (QA), las cuales se condicionan a las necesidades de los usuarios, garantizando sistemas más eficientes, confiables y seguros para que la experiencia de sus usuarios sea la mejor.

Actualmente, la empresa no cumple con los estándares requeridos en "seguridad informática", debido a que, no están certificados sobre el estatuto ISO 27001 de 2022, y solo están cumpliendo con el anexo A de dicha norma, lo que es insuficiente ya que se están exponiendo a una pérdida de información sensible tanto de sus propios funcionarios como de sus clientes, esto conllevaría que los socios y/o accionistas pierdan confianza, y en casos de alta gravedad (cuando hay pérdida de información), se expondrían a sanciones administrativas.

Teniendo en cuenta lo anteriormente plasmado, surge el interrogante que genera la pregunta de investigación: ¿Es posible que, realizando una consultoría a los controles en seguridad informática en SQA S.A., contribuya a lograr una certificación en el estatuto ISO27001 de 2022, y así mitigar las vulnerabilidades tecnológicas que puedan afectar a la empresa?
(SQA, 2023)

Objetivo General

Proponer un procedimiento que identifique las falencias en las normas, estatutos y controles en seguridad de la información, sobre la empresa SQA S.A, y así facilitar ser certificada en la norma ISO:27001 de 2022.

Objetivos Específicos

- Proponer un método que diagnostique las falencias en las políticas de seguridad de la información, sobre la empresa SQA S.A, según la norma ISO:27001 de 2022.
- Proponer un método que identifique las falencias en los controles de seguridad de la información, sobre la empresa SQA S.A, fundamentada en la norma ISO:27001 de 2022.

- Establecer acuerdos y definir responsabilidades, con el fin de especificar las funciones a realizar por parte de las personas involucradas en las áreas relacionadas con el SGSI.

Alcances

Con esta consultoría se pretende brindar a la empresa un procedimiento, que al ser implementado por los empleados identifique las falencias en sus políticas y controles de seguridad de la información, por otro lado, se brinda un diagnóstico actual del estado de sus políticas, como también se sugiere un método para Analizar y mitigar los riesgos a los que se encuentra sometido el sistema de información en la empresa SQA S.A, dicho método estará basado en los procesos de evaluación y control de la norma ISO 27001:2022, lo que brinda seguridad y confiabilidad.

Limitaciones

1. Recursos financieros

Las limitaciones financieras pueden afectar los procesos para lograr la certificación en el ISO/IEC 27001:2022 ya que se debe contar con un presupuesto para la evaluación de dicha ISO por medio de una empresa y/o contratista certificado que realice la consultoría.

2. Recursos humanos

Esta limitación pretende dar a entender que la certificación de la ISO/IEC 27001:2022 solo puede lograrse mediante la colaboración y compromiso de los colaboradores de la empresa SQA S.A. por ejemplo el cumplimiento en las normas, estatutos y controles en seguridad de la información.

3. Tamaño empresa

Esta propuesta abarca únicamente la empresa SQA S.A. en su situación actual por lo que no se abordaran casos específicos donde el número de colaboradores y/o sucursales en otras partes del mundo.

1. Marco teórico

1.1 Sistema de información

Un sistema es un grupo conformado por objetos que actúan entre ellos mismos, para lograr un objetivo específico.

Los sistemas pueden ser abiertos o cerrados, físicos o intangibles. En relación a la información, Morales lo define como: un conjunto organizado en contenidos y servicios, a partir de tecnologías digitales y en red los cuales, una industria pone a disposición de seres pensantes, interesados en dicha tecnología, para disminuir la dificultad en la producción y el gasto, en grupos estructurados y específicos de datos, guiados a transformarse en información de gran importancia para dicha industria.

(Morales, 2013)

1.2 Sistemas en Gestión de Seguridad informática SGSI:

Este conjunto puede apercibirse como un tipo de herramienta de bajo valor monetario, la cual cualquier PYME, puede llegar a utilizar. Esta norma facilita la establecencia de estatutos, procesos y controles, con el fin de limitar y prevenir los posibles riesgos de la empresa. El hecho de implementar la certificación ISO, modifica totalmente el desempeño y las funcionalidades de dicha empresa, con el objeto de que éstas sean completamente optimizadas.

Dicha herramienta permite evaluar los posibles riesgos que se puedan presentar en el funcionamiento de la empresa, gestionándolos de forma efectiva: adicionalmente, permite analizar lo que dicha organización necesita en relación a la protección se su activo más preciado reflejado en salvaguardar su propia información.

(Ochoa, 2023)

1.3 ¿Por qué Implementar un SGSI?

Administrar la seguridad en una empresa resulta vital, ya que su información es uno de los activos más importantes; al implementar un Sistema de gestión en seguridad informática, y saber gestionarlo eficientemente:

- se disminuyen los riesgos y costos
- se da una mejora continua en los procesos de red
- se establecen dominios idóneos en la seguridad informática
- Se da una fácil integración, en función de los estatutos anteriores, a la actual normativa ISO 27001
- se mejora el nivel competitivo, en relación a empresas que no cuentan con la certificación adecuada y/o actualizada

1.4 Norma ISO 27001

Este conjunto de reglas garantiza las prácticas óptimas en relación a la seguridad informática, estableciendo requerimientos necesarios para salvaguardar los preciados bienes y/o activos de la información, aplicando así los dominios apropiados, para llegar a asegurar la protección de dichos bienes, según los requerimientos de la empresa, y poder así implantar con éxito un SGSI.

La norma ISO 27001 de 2022, es manejada a nivel mundial, la cual define los criterios para un SGSI (Sistema de Gestión de Seguridad de la Información). Este estándar ofrece estructuras completas, aplicadas hacia el análisis, categorización y la disminución de los riesgos, asociados a seguridad informática en una organización; por esta razón, resulta primordial contar con esta certificación, ya que de otro modo las entidades u organizaciones pueden verse afectadas por ciberataques, perdiendo clientes, empleados, daño a la imagen corporativa, perdida de información privada e incluso sanciones.

1.5 Beneficios de la ISO 27001 de 2022

- Reducir los factores que disminuyen la seguridad: se garantiza tener todos los datos protegidos sin importar su ubicación
- Ayuda a organizar la información de la empresa
- Planificación adecuada
- Intercambio seguro de la información
- Posición competitiva
- Reputación de la empresa
- Cumplimiento de las regulaciones

- Ayuda a tener un entorno de trabajo seguro
- Ahorro de tiempo y diseño.

2. Diseño Metodológico

2.1 Desarrollo objetivo 1.

Se sugiere a la empresa SQA S.A adoptar e implementar la metodología "Scrumban", de forma continua en los conjuntos laborales, para llegar a realizar auditorías interiores, las cuales se den a través del "SharePoint" de la empresa (Office 365); este es el caso del software libre, el cual no requiere de un permiso o licencia, ni lago alguno para su uso; esto evita un gasto significativo en software, alineando así el objetivo de contar con los recursos necesarios para la propuesta de implementación del SGSI, teniendo en cuenta siempre, el cumplimiento de los estatutos contenidos en la norma ISO/IEC 27001 de 2022, junto a los lineamientos dados hacia la seguridad informática, dados durante todas las etapas de certificación.

2.2 Desarrollo objetivo 2.

Se propone la separación de un intervalo de tiempo, dentro del cronograma diario, de las personas responsables e interesadas del progreso en el seguimiento en los controles aplicados a la seguridad en la información. Posterior a la finalización del proceso de separación del intervalo de tiempo, se registra un "checklist" a partir de los controles alcanzados, proporcionando así, un registro histórico en la revisión, y en la evidencia misma del control ajustado.

2.3 Desarrollo objetivo 3.

Sugerir la alta dirección de SQA S.A en la elaboración de roles y responsabilidades, con el propósito de identificar las tareas asignadas a los participantes en las diversas áreas dentro de la empresa. Esto permitirá asegurar el cumplimiento de los requisitos establecidos en la propuesta de SGSI, para la

preparación de la ISO, se recomienda usar una plantilla de uso periódico con buenas prácticas donde se van a revisar los siguientes ítems:

- Establecer la metodología de trabajo a partir de los estándares existentes en ISO 27001, considerando los objetivos y necesidades particulares de SQA S.A.
- Asignar roles y responsabilidades, incluyendo la designación de un Oficial de Seguridad de la Información (ISO).
- Generar una estructura organizada que contemple los controles y evidencias necesarios para respaldar la implementación del SGSI.
- Evaluar y verificar las políticas y controles de seguridad de la información implementados en SQA S.A mediante auditorías internas y revisiones periódicas.
- Realizar análisis de riesgos de manera regular para asegurar la efectividad continua del SGSI y su alineación con los objetivos de la empresa.
- Iniciar acciones preventivas y correctivas basadas en los resultados de las auditorías y evaluaciones del SGSI.
- Facilitar la capacitación continua del personal en relación con las políticas y controles de seguridad de la información establecidos.

3.Resultados

Se presenta un documento de consultoría robusto a la empresa SQA S.A, en donde se pretende contribuir al avance en la investigación y el proceso de certificación, en la reglamentación ISO 27001 de 2022. De igual forma se realizó un análisis detallado de la documentación aportada, que, ayudará eficientemente a que la empresa continúe por un camino favorable hacia poder lograr dicha certificación.

4. Conclusiones y recomendaciones

4.1 Conclusiones

Se destaca la importancia en la implementación del SGSI en la organización SQA S.A, para gestionar y controlar eficazmente los riesgos asociados a la seguridad informática. La propuesta de consultoría se centra en la norma ISO 27001:2022, adaptándola a las necesidades específicas de dicha organización, garantizando así la protección de la información sensible y la continuidad del negocio.

Se aconsejable la actualización de los controles en el anexo A, inicialmente contenido en la reglamentación ISO 27001 de 2013, para mutar al Anexo A, de la reglamentación ISO 27001 de 2022. Adicionalmente se deben revisar los 94 controles de la norma ISO 27001 de 2022, reuniendo todos los requisitos necesarios, para poder aplicar a la certificación como tal.

4.2 Recomendaciones

Como recomendaciones para la propuesta de una Implementación de una Consultoría en la Gestión de la Seguridad de la Información (SGSI), basados en la Norma ISO/IEC 27001:2022 para obtener la Certificación en la empresa SQA S.A, se deben:

- Asignar recursos financieros adecuados para la implementación y **mantenimiento** del SGSI, considerando la contratación de expertos certificados.
- Involucrar activamente a todo el personal en la capacitación sobre políticas y controles de seguridad de la información.
- Realizar auditorías internas de manera regular para evaluar la efectividad del SGSI y realizar ajustes según sea necesario.
- Mantenerse actualizado sobre cambios en la norma ISO 27001:2022 y ajustar el SGSI en consecuencia.

Lo anterior proporciona un marco sólido para la implementación exitosa del SGSI en SQA S.A, contribuyendo a su certificación en la norma ISO 27001:2022 y mitigando los riesgos de ciberseguridad que puedan afectar a la empresa.

Bibliografía

bsigroup. (18 de 11 de 2023). *Obtenido de Casos de éxito de Gestión de ISO/IEC 27001.* Obtenido de bsi: https://www.bsigroup.com/es-CO/seguridad-de-la-informacion-isoiec-27001-/casos-de-exito-de-gestion-de-isoiec-27001/

GERALDINE ORTIZ, L. E. (2018). *UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS.* Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/13419/Geraldine%20Alejandra?sequence=4

Gómez, I. R. (8 de 11 de 2023). *UDEMY*. Obtenido de 6. Cambios de la versión 2013 a la 2022: https://tcsglobal.udemy.com/course/iso-iec-27001/learn/lecture/39606554#overview

ISO 27001. (8 de 11 de 2023). Obtenido de ¿POR QUÉ IMPLANTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN?: https://normaiso27001.es/

Morales, J. C. (2013). *Sistema de información de la empresa.* Barcelona: www.editorialuoc.com.

Ochoa, A. (8 de 11 de 2023). *Importancia de las Normas Iso*. Obtenido de Udemy: https://tcsglobal.udemy.com/course/aprende-iso-27001/learn/lecture/8133282#overview

Ochoa, A. (08 de 11 de 2023). *6. Seguridad*. Obtenido de Udemy: https://tcsglobal.udemy.com/course/aprende-iso-27001/learn/lecture/8147446#overview

Services, T. T. (2023). *TCS Governance, Risk, and Compliance Services*. Obtenido de Data & Cybersecurity for Robust Defense Against Cyber Attacks: https://www.tcs.com/what-we-do/services/cybersecurity/solution/governance-risk-compliance-security-services

SQA, S. Q. (2023). *sqasa*. Obtenido de https://sqasa.co/privacy-policy/