Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Implantación de un sistema de gestión integrado con las normas ISO/IEC 27001:2013 e ISO/IEC 20000-1:2018

Trabajo Fin de Máster

Máster Universitario en Ingeniería Informática

Autor: Aburto Zamora, Keith Yasira

Tutor: Boza García, Andrés

Tutora: Gordo Monzó, Mari Luz

2019-2020

Dedicatoria

Dedico este trabajo con todo mi cariño a mi familia; de manera especial a mi querida Madre por ser un pilar y referente en mi vida.

A mi amado esposo, eres mi inspiración y mi motivación.

A la memoria de G.S.R.A., tu recuerdo siempre presente en nuestro corazón.

Agradecimientos

Después de un intenso período de esfuerzo y aprendizaje escribo este apartado para finalizar mi trabajo fin de master y agradecer a todas las personas que me han apoyado durante el camino recorrido hasta ahora, y que estuvieron conmigo en los momentos de alegrías y angustias

En primer lugar, me gustaría darles las gracias a mis tutores A. Boza y M. Gordo, por el tiempo dedicado, vuestra valiosa ayuda y enseñanzas brindadas, sin las cuales no hubiese sido posible culminar este trabajo. Un especial agradecimiento a la profesora M. Cuenca por todo el apoyo que me ha otorgado, así como también por la motivación para finalizar mis estudios.

A todos mis compañeros y amigos, que de alguna manera han colaborado en la realización de este proyecto, en especial A. Romero por estar siempre a mi lado y por su gran apoyo, necesario en los momentos difíciles de este trabajo y esta profesión.

A mi familia, que ha sido un soporte durante este proceso, les agradezco por aconsejarme en todo momento, por los valores y principios que me han inculcado.

A mi madre, por su amor, trabajo y sacrificio en todos estos años, gracias a su apoyo incondicional he llegado a culminar esta etapa de mi vida.

A mi marido, su ayuda y aportes han sido fundamental para el desarrollo de mi trabajo, gracias por tu infinita paciencia, por motivarme en los momentos de debilidad y flaqueza, este trabajo también es tuyo.

Muchas gracias a todos.

Resumen

La información es un recurso clave para todas las empresas, los sistemas de información cada vez más están expuestos a amenazas, que pueden vulnerar los activos críticos de información, como la pérdida o robo de datos causada por usuarios no autorizados, incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la empresa, y denegación de servicio por ciberataques.

La gestión de la seguridad de la información permite establecer un marco con políticas y procedimientos que ayudan a la seguridad frente a incidentes causados por un ataque. Los procesos de negocio están relacionados con los sistemas de información, la implementación de la gestión de servicios TI, permite tener el control de las actividades, el uso eficiente de los sistemas, y ayuda a mejorar el nivel de servicio proporcionado, asegurando la entrega y calidad de estos.

Las estrategias de transformación digital son un recurso poderoso que ayudan a las empresas en los procesos de negocio para aumentar la competitividad y permitir la innovación, las certificaciones ayudan a generar fiabilidad y demostrar calidad en los procesos internos y servicios que ofrecen las empresas.

La Norma ISO/IEC 27001 permite el aseguramiento, confidencialidad, e integridad de la información y de los sistemas que la procesan.

La Norma ISO/IEC 20000-1 establece los requisitos para la prestación de servicios de TI, ayuda a las organizaciones a medir los niveles de servicios y evaluar su desempeño.

La Norma ISO/IEC 27013 es una guía para la implementación integrada de un Sistema de Gestión del servicio (SGS) según la norma ISO/IEC 20000-1 y un Sistema de Gestión de la Seguridad de la Información (SGSI), según la norma ISO/IEC 27001.

En este Trabajo de Fin de Máster (TFM), se analiza la Norma ISO 27013 para establecer un Sistema Integrado de Gestión (SIG) que facilite la implantación conjunta de las normas ISO/IEC 27001 e ISO/IEC 20000-1, con el objetivo de simplificar el desarrollo y mantenimiento, reduciendo los costes y tiempos. Se implantarán las normas desde cero en una empresa de servicios. Además, se realizará el desarrollo de una herramienta informática que facilitará la toma de información de la auditoría inicial de los sistemas de información.

Palabras clave: Tecnologías de la información, Seguridad de la Información, Gestión de Servicios TI, ISO/IEC 27001, ISO/IEC 20000-1, ISO/IEC 27013.

Abstract

Information is a key resource for all companies, the Information systems are frequently exposed to various types of threats which can cause different types of damages, such as data loss, security incidents, and denial of service due to cyber-attacks.

Information security management allows the establishment of policies and procedures that help security against incidents caused by an attack. Business processes are related to information systems, IT service management allows control of activities, helps improve the level and quality of services.

Digital transformation strategies are a powerful resource that help companies to increase competitiveness and enable innovation, certifications help to generate reliability and demonstrate quality in internal processes.

ISO/IEC 27001, Information security management systems. Information security is the protection of information to ensure Confidentiality, Integrity and Availability.

ISO/IEC 20000-1, Service Management System Requirements. Service management system is a management system to direct and control the service management activities of the service provider.

ISO/IEC 27013:2015 provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.

In this master's thesis, ISO 27013 standard is analyzed. Integrated management systems provide a framework for organizations to combine a number of international standards related to their area of operation, in order to simplify the development and maintenance, reducing cost and time. In addition, a tool will be developed to facilitate the taking of information from the initial audit.

Keywords: Information Technology (IT), Information Security, IT Service Management, ISO / IEC 27001, ISO / IEC 20000-1, ISO / IEC 27013.

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Actualmente, es preciso para las empresas contar con una certificación para satisfacer los requisitos de los clientes, optimar sus procesos, mejorar la imagen corporativa y posicionarse como una empresa eficaz y confiable en el mercado globalizado. Los incidentes de seguridad afectan el impacto organizacional y financiero, cuando las empresas han sido víctimas de un ataque, los daños operacionales y pérdidas económicas son muy perjudiciales, los ciberataques se han convertido en un problema para las empresas, estas pueden perder fiabilidad y ventaja competitiva, por tanto, la gestión de la seguridad de la información es responsabilidad del gobierno de TI no solo del departamento de TI.

El gobierno de la seguridad de la información permite establecer un marco con políticas y procedimientos que ayudan a gestionar la seguridad frente a incidentes causados por un ataque. El objetivo de este trabajo es diseñar un modelo de buenas prácticas para las empresas, que garantice la integridad de la información, tomando como referencia la Normativa ISO/IEC 27013, para incorporar las funciones de seguridad de la información con las funciones de gestión de los servicios, y de esta manera optimizar los recursos dedicados a la implementación y mantenimiento del sistema de gestión.

La Norma ISO/IEC 20000-1 para gestión de servicios de TI y la Norma ISO/IEC 27001 para la seguridad de la información proporcionan una serie de capacidades, tales como la reducción de los incidentes de seguridad, una mejor toma de decisiones con conocimiento del riesgo y soporte mejorado a la competitividad. Dichas normas tienen procesos y actividades similares, incluido el proceso iterativo dirigido a una mejora continua y adaptado a las vulnerabilidades y amenazas constantes, es decir a los cambios externos de ataques y violaciones de seguridad.

Este trabajo de fin de Master se enfoca en tres estándares específicos:

- ISO/IEC 27013:2015. Tecnologías de la información – Técnicas de Seguridad - Guía para la aplicación integrada de la norma ISO/IEC 27001 e ISO/IEC 20000-1.
- ISO/IEC 27001:2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos
- ISO/IEC 20000-1:2018. Tecnologías de la información - Gestión de Servicios - Parte 1: Requisitos del Sistema de Gestión de Servicios.

En primer lugar, debemos definir el estado actual de la empresa, para detectar las debilidades y deficiencias. Una vez se conoce la situación actual debemos alinear los objetivos de seguridad con los de servicios TI, para priorizar las necesidades y realizar un plan de acciones que se

adapte a las circunstancias particulares de la empresa, y así contar con un sistema compuesto de procesos y documentos de apoyo como políticas y procedimientos para la gestión de la seguridad de la información y la gestión de servicios TI.

1.1. Problemática

Las estrategias de transformación digital son un recurso poderoso que ayudan a las empresas en los procesos de negocio para aumentar la competitividad y permitir la innovación, la seguridad de la información es de vital importancia para proteger los datos, el activo crítico que debe ser gobernado correctamente, ya que estas tecnologías aumentan las vulnerabilidades de seguridad.

La ciberseguridad en el contexto de la seguridad de la información acompaña a todas las medidas de protección frente a ataques intencionados, violaciones e incidentes de seguridad y debe estar alineada con la gobernanza y la gestión.

Cada año aumenta el número de empresas que han sufrido un incidente de seguridad. El número de amenazas y vulnerabilidades han crecido exponencialmente y se han vuelto más complejas. En 2019, el CCN-CERT[1] gestionó 42.997 ciberincidentes.

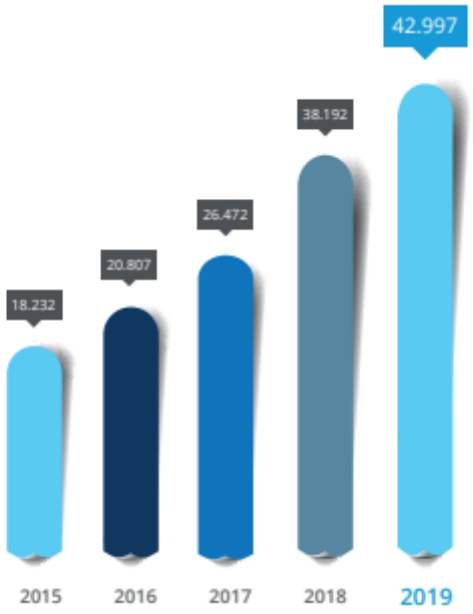


Figura 1. Incidentes gestionados por el CCN-CERT entre 2015 y 2019

Nota. Fuente: IA, 13/20 Ciberamenazas y Tendencias 2020. Informe de amenazas del CCN-CERT, 15.

[1] CCN-CERT Centro Criptológico Nacional Computer Emergency Response Team

Los Ciberincidentes detectados han afectado a múltiples sectores, los tipos de incidentes gestionados por el CCN-CERT en 2019 son:

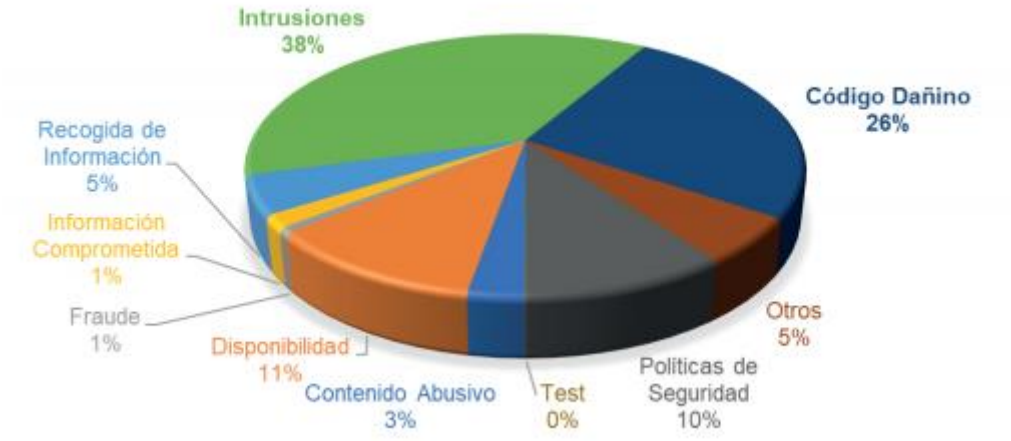


Figura 2. Incidentes gestionados en 2019 por el CCN-CERT por tipología

Nota. Fuente: IA, 13/20 Ciberamenazas y Tendencias 2020. Informe de amenazas del CCN-CERT, 16.

- Código dañino: troyanos, spyware, etc.
- Seguridad de la información: violaciones de políticas de seguridad
- Contenidos abusivos: contra la imagen
- Disponibilidad: daños de imagen y productividad
- Fraude: propiedad intelectual, protección de datos o suplantación de identidad.
- Información comprometida: acceso y exfiltración y/o borrado y publicación de información no publica
- Recogida de información: primeros pasos para una campaña mayor
- Intrusiones: ataques dirigidos

A continuación, se muestra los agentes de las amenazas en las empresas y la tipología de sus acciones.

Tabla 1

Agentes de las amenazas

Actores de las amenazas	Tipos de amenazas a las Empresas	Descripción
Estados y grupos patrocinados por Estados	Espionaje Manipulación de Sistemas	El objetivo perseguido por este tipo de ataques es sustraer información (espionaje), interrumpir la prestación de servicios esenciales (sabotaje) e influir en la opinión pública de los países atacados
Delincuentes	Robo de información Manipulación de la información Interrupción de servicios Manipulación de sistemas	El objetivo perseguido es la comisión de ciertos delitos (p. ej. Tarjetas de crédito), robo de identidad (credenciales), suplantación, espionaje, etc.
Hacktivistas	Interrupción de servicios Robo de información Manipulación de información	El objetivo perseguido es desarrollar operaciones de protesta para llamar la atención de los medios, sin perseguir la monetización de sus acciones
Personal Interno	Interrupción de servicios Robo de información	Este grupo está formado por personas maliciosas y/o negligentes (usuarios de sistemas, usuarios privilegiados, proveedores, etc.). La mayor parte del daño parece ser causado por acciones no intencionadas.

Nota. Fuente: Adaptado de IA, 13/19 Ciberamenazas y Tendencias 2019. Informe de amenazas del CCN CERT, 14.

Los daños causados por las brechas de seguridad son un tema importante en las empresas, los ataques a los sistemas de información son más peligrosos, y se producen muchos incidentes relacionados con:

- la computación en la nube, gran cantidad de datos de las empresas están en la nube;
- los empleados, el eslabón más débil en la seguridad informática;
- los dispositivos conectados a internet vía WIFI;
- ordenadores con sistemas operativos sin actualizaciones ni parches de seguridad.

Lo anterior pone de manifiesto que las empresas necesitan contar con un modelo de sistema de gestión para mitigar los riesgos y dar respuesta rápida a los posibles problemas de seguridad, prevenir futuros fallos o interrupciones de los servicios.

1.2. Motivación

La elección del tema y elaboración de este trabajo representa un complemento en mi desarrollo y desempeño profesional. Una de las motivaciones que llevó a realizar este trabajo, es debido a las necesidades y los desafíos que actualmente afrontan las organizaciones, respecto a la problemática que afecta la seguridad de la información y calidad de los servicios que ofrecen. Hoy por hoy, existen pocos estudios dedicados a los Sistema Integrados de Gestión, indispensables para la toma de medidas que aseguren el buen desempeño y funcionamiento de los procesos, satisfagan las necesidades de los clientes, cumplan con los requisitos legales y les permita a las organizaciones ser más competitivos.

Dada la tendencia actual en las certificaciones de seguridad y gestión de los servicios, este Trabajo de Fin de Máster (TFM), está diseñado para implantar un Sistema de Gestión Integrado en una organización que no cuenta con ningún sistema de gestión previo, con la finalidad de obtener beneficios de eficiencia y eficacia de las normas, reduciendo los esfuerzos y maximizando los recursos disponibles en la organización.

La realización de este trabajo consiste en el análisis de deficiencias con una aplicación web, que permitirá la automatización de los Sistemas de Gestión, ya que hoy en día en el mercado es difícil encontrar una herramienta especializada con estas características. Tras la finalización de este proyecto, se espera ayudar en la evaluación de requisitos de cada norma de forma conjunta, facilitando el trabajo de los consultores, auditores y organizaciones.

1.3. Objetivos

El objetivo general del presente trabajo es desarrollar una herramienta informática que ayude en la fase inicial de la implantación de un Sistema Integrado de Gestión (SIG), de las Normas ISO/IEC 27001 e ISO/IEC 20000-1, para diagnosticar el nivel de madurez de los procesos de gestión de servicios de TI y los controles de seguridad de la información, y priorizar las actividades en la implantación de las normativas, logrando así reducir los esfuerzos necesarios y optimizar los costes de la organización.

Para alcanzar este objetivo es preciso cumplir con los siguientes objetivos específicos:

- Utilizar como referencia la Norma ISO/IEC 27013:2015, para analizar los procesos de gestión de servicios de TI de la Norma ISO/IEC 20000 y los controles de seguridad de la información de la Norma ISO/IEC 27001.

- Elaborar un mapa de relaciones entre los controles de la Norma ISO/IEC 20000 e ISO/IEC 27001, para identificar los requisitos comunes que conforman el sistema integrado de gestión.

- Determinar el método de integración a aplicar en la implantación de las normas ISO/IEC 27001 y Norma ISO/IEC 20000, con las diferentes alternativas existentes para desarrollar el sistema integrado de gestión.

- Establecer el plan de integración para implantar el sistema integrado de gestión de las normas ISO/IEC 27001 y Norma ISO/IEC 20000, en una empresa de servicios cloud, utilizando la herramienta desarrollada para el análisis de deficiencias.

1.4. Estructura

El trabajo consta de 7 capítulos y los Anexos que se muestran a continuación:

Capítulo 1. Introducción: En este capítulo se presentan los problemas de ciberseguridad y los agentes de las amenazas que afectan la seguridad de la información en las empresas, los motivos que han llevado a realizar la investigación y se describen los objetivos que se pretende conseguir con este trabajo.

Capítulo 2. Estado del arte. En primer lugar, se realizará una descripción del gobierno de TI, ciberseguridad, seguridad de la información y análisis de riesgos. Una vez definidos los conceptos previos y la problemática existente en materia de seguridad, se efectuará un estudio de los estándares para la gestión de la seguridad de la información y la gestión de servicios TI. Además, se describe el sistema integrado de gestión propuesto por la norma ISO/IEC 27013. Finalmente, se presenta los lenguajes de programación web, para el desarrollo de la herramienta.

Capítulo 3. Análisis del problema. Se mostrarán las posibles soluciones que se consideran para implantar un sistema integrado de gestión. En cuanto al desarrollo de la herramienta, se presentará el análisis de requisitos del software para especificar claramente lo que debe cumplir la herramienta.

Capítulo 4. Solución propuesta. En base a los resultados del capítulo anterior, se planteará una propuesta para elaborar un modelo de implantación del sistema integrado de gestión. Una vez identificados los requisitos de la herramienta, se mostrará el diseño de la base de datos y la tecnología utilizada para llevar a cabo el desarrollo de la misma.

Capítulo 5. Implantación del Sistema Integrado de gestión. Se expondrá un caso práctico aplicado a una empresa de servicios cloud, con los pasos que se han elaborado para implantar el sistema integrado de gestión. Asimismo, se pondrá en marcha la herramienta desarrollada para obtener los resultados del análisis de la situación actual en la organización.

Capítulo 6. Conclusiones. Se presentarán las conclusiones y los posibles trabajos a futuro que se puedan abordar para mejorar y ampliar las funcionalidades del trabajo realizado

Capítulo 7. Referencias. Se recogerán las referencias consultadas para la elaboración de este trabajo.

Anexos. Se presentarán el resumen de las normativas, el manual de usuario de la aplicación y un ejemplo de los resultados del análisis de deficiencias realizado con la aplicación.

2. Estado del arte

2.1. Gobierno y seguridad de la información

¿Qué es la ciberseguridad?

Según ISACA[2], la definición de Ciberseguridad es:

> "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

En la seguridad de la información el foco se encuentra en las amenazas avanzadas. Las amenazas persistentes avanzadas (APT), son ataques, infiltraciones y violaciones de seguridad con un nivel de esfuerzo importante en términos de tiempo e inversión, otras amenazas relevantes incluyen el activismo político, piratería y daño reputacional empresarial.

Los ciberincidentes no poseen las mismas características, la siguiente tabla muestra una clasificación que ha hecho el CCN-CERT:

¿Qué es gobierno?

Gobierno se deriva del verbo griego kubernáo que significa dirigir, es decir, un sistema que permite a las empresas establecer una dirección y supervisar los objetivos.

COBIT 5 define el gobierno como:

> El gobierno asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar los objetivos de empresa acordados y equilibrados que han de ser alcanzados; establecer la dirección mediante la priorización y toma de decisiones; y supervisando el rendimiento y el cumplimiento respecto a la dirección y objetivos acordados.

El buen gobierno TI forma parte del buen gobierno corporativo, ambos deben operar sincrónicamente, para equilibrar la competitividad y productividad de las empresas, garantizando un desarrollo y crecimiento sostenible a largo plazo.

[2] ISACA - Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)

Gobierno TI

El Gobierno de TI es parte del Gobierno corporativo, ayuda a evaluar y monitorizar el uso de las TI para cumplir con las metas empresariales.

Jan van Bon (2010) define el gobierno de TI como:

> El Gobierno de TI consiste en un completo marco de estructuras, procesos y mecanismos relacionales. Las estructuras implican la existencia de funciones de responsabilidad, como los ejecutivos y responsables de las cuentas de TI, así como diversos Comités de TI. Los procesos se refieren a la monitorización y a la toma de decisiones estratégicas de TI. Los mecanismos relacionales incluyen las alianzas y la participación de la empresa/organización de TI, el dialogo en la estrategia y el aprendizaje compartido.

El Gobierno TI está dentro del dominio de la gestión de la información y garantiza que las tecnologías de la información soportan la estrategia de la empresa y las metas corporativas.

Seguridad de la Información

ISACA define seguridad de la información como:

> Asegurar que, dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (Integridad) y su falta de acceso cuando se la necesita (disponibilidad).

Según la Norma ISO/IEC 27002:

> Seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Los principios de la seguridad de la información comunican las reglas de la empresa para apoyar los objetivos de gobierno y los valores empresariales. En 2010, ISACA junto a otras organizaciones líderes en seguridad de la información desarrollaron principios que ayudarán a añadir valor mediante la promoción de buenas prácticas. Estos principios están estructurados para dar soporte a tres tareas: soporte al negocio, defender el negocio y promover un comportamiento responsable en seguridad de la información.

2.2. Estándares y Normas para la gestión de la seguridad de la Información

En la actualidad la gran dependencia de los sistemas de información y el panorama actual de ciberamenazas, hace que las Normas para la gestión de la seguridad de la información adquieran un papel importante.

Por otra parte, contar con un Sistema de Gestión de Seguridad de la Información (SGSI) facilita a las empresas cumplir con requerimientos legales y contractuales relacionados con la seguridad de la información. Por ejemplo, el Reglamento General de Protección de datos. También se reducen los riesgos, ya que permite establecer controles o medidas de seguridad para la mitigación de los mismos. Aumenta la confiablidad y mejora la competitividad, asegurando el correcto funcionamiento de las plataformas de acceso a la información.

ISO/IEC 27000

La Organización Internacional de Estandarización, a través de las normas recogidas en ISO/IEC 27000, establece un modelo de la seguridad de la información. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI.

2.3. Estándares y Normas para la gestión de servicios TI

La gestión correcta de los servicios de TI nos ayuda a centralizar y simplificar los procesos que se llevan a cabo, mejorando la productividad, permitiendo la calidad de los servicios y fiabilidad de los sistemas. Asimismo, permite alinear la estrategia tecnológica con los procesos de negocio, de acuerdo con el nivel de servicio pactado con el cliente.

Existen múltiples estándares para proveer y gestionar de formar eficaz las actividades esenciales para que los departamentos de TI puedan prestar servicios optimizados y alineados con las necesidades de las empresas, a continuación, se realiza una descripción de las Normas más reconocidas:

Infraestructura de Tecnología de la Información (ITIL)

La Biblioteca de la Infraestructura de Tecnología de la Información (ITIL), está formada por una serie de “Mejores Prácticas” procedentes de todo tipo de suministradores de servicios de TI.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización.

El rol y los sistemas de provisión de información han cambiado y crecido desde el lanzamiento de la versión 2 de ITIL (en febrero de 2000). TI forma parte de servicios a los que da soporte. La versión 3 de ITIL pretende facilitar la comprensión del nuevo papel de la TI con toda su complejidad y dinamismo. Para ello se ha elegido un nuevo método de Gestión de Servicios que no se centra en los procesos, sino en el Ciclo de Vida del Servicio.

El Ciclo de Vida del Servicio es un modelo de organización que ofrece información sobre:

- La forma en que está estructurada la gestión del servicio.
- La forma en que los distintos componentes del Ciclo de Vida están relacionados entre sí.
- El efecto que los cambios en un componente tendrán sobre otros componentes y sobre todo el sistema del Ciclo de Vida.

Modelo de madurez: CMMI

En el sector de TI, el proceso de mejora de madurez de procesos se conoce especialmente en el contexto del Modelo de Madurez de la Capacidad Integrado (CMMI). Este método de mejora de procesos fue desarrollado por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon.

CMMI es un modelo continuo a la vez que por etapas. En la representación continua, la mejora se mide utilizando niveles de capacidad, mientras que la madurez se mide para un proceso concreto en una organización. En la representación por etapas, la mejora se mide utilizando niveles de madurez para un conjunto de procesos en una organización.

El modelo de representación por etapas de CMMI define cinco niveles de madurez designados por los números del 1 al 5, cada uno de los cuales sirve de base para la siguiente fase en la mejora continua del proceso:

- Inicial: Procesos específicos y caóticos.
- Gestionado: Los proyectos de la organización garantizan que los procesos se planifican y ejecutan según la política de la organización.
- Definido: Los procesos están bien caracterizados y documentados y se describen en estándares, procedimientos, herramientas y métodos.
- Gestionado cuantitativamente: La organización y sus proyectos establecen objetivos cuantitativos de calidad y rendimiento de procesos y los utilizan como criterios para la gestión de procesos.
- Optimización: Se centra en la mejora continua del rendimiento de los procesos a través de mejoras incrementales e innovadoras de procesos y tecnologías.

ISO/IEC 20000

Las Normas ISO/IEC 20000 se componen de un conjunto de procesos que interactúan entre sí y que son necesarios para la prestación de un servicio con el objetivo de normalizar la gestión de los sistemas de información mediante procesos eficaces que articulen todas las actividades de la organización de TI hacia un claro enfoque al servicio y al cliente.

Además de los procesos contemplados en la norma, hay otras disciplinas que hay que tener en cuenta para lograr la excelencia del proveedor de TI, como son:

- La alineación de TI con las necesidades del negocio.
- La gestión de la demanda de las necesidades del negocio
- La planificación de la cartera anual de proyectos.
- La madurez de los procesos de desarrollo y sus metodologías.
- El imprescindible conocimiento técnico.
- La arquitectura de las aplicaciones y de la infraestructura.
- La renovación de las infraestructuras.
- La calidad de los proveedores y de los servicios contratados.
- El liderazgo de la dirección, la motivación del personal, etc.

2.4. Sistema Integrado de Gestión (SIG)

Cuando una organización establece varios sistemas de gestión necesita coordinarlos eficazmente, haciéndolos compatibles entre sí de forma que se puedan establecer objetivos alineados, se obtenga una visión global de los sistemas y se facilite la toma de decisiones. En los sistemas de gestión hay ciertos elementos comunes que se pueden gestionar de forma integrada y ciertos elementos que son específicos de la cada norma.

2.5. Soluciones tecnológicas de Gobierno

Una solución de IT para Gobierno, Riesgo y Cumplimiento (GRC), permite gestionar los requisitos normativos y automatizar la documentación de cumplimiento, existen muchas soluciones en el mercado tales como:

- IBM OpenPages GRC Platform
- MetricStream
- SAP GRC Audit Management

2.6. Documentos relacionados

Se ha realizado una búsqueda de trabajos relacionados con el gobierno, la seguridad de la información, los sistemas integrados de gestión en los sitios Riunet y Google académico que se presentan a continuación:

Tabla 2

Búsqueda de documentos en Riunet y Google académico

TITULO	**AUTOR**	**INSTITUCIÓN**	**AÑO**
El papel del informático como Auditor en la "ISO 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas De gestión de la seguridad de la Información. Requisitos."	Jorge Asensi Shaw	Universidad Politécnica de Valencia Trabajo fin de grado	2018-2019
Las normas de gestión de empresas y su aplicación a las	Adrián Martínez Rochina	Universidad Politécnica de Valencia	2018-2019

empresas informáticas. La auditoría y la certificación de empresas		Trabajo fin de grado	
COBIT 5 y el Cuadro de Mando Integral como herramientas de Gobierno de TI	Roberto Monfort Casañ	Universidad Politécnica de Valencia Trabajo fin de grado	2015-2016
Relación entre gobierno de tecnologías de la información y Resultados del sistema sanitario en hospitales del servicio Madrileño de salud	Juan Carlos Muria Tarazón	Universidad Politécnica de Valencia Tesis doctoral	2015
Estudio de una metodología de trabajo para la realización de auditorías integradas de sistemas de información	Eloy Millet Colomar	Universidad Politécnica de Valencia Trabajo fin de grado	2014-2015
Diseño de una herramienta de BI (Business Intelligence) basada en Excel para el análisis de indicadores de competitividad empresarial	José Juan Miret Conejero	Universidad Politécnica de Valencia Trabajo fin de grado	2014

Modelo de aporte de valor de la implantación de un Sistema de gestión de servicios de ti (SGSIT), basado en Los requisitos de la norma ISO/IEC 20000	Mª Carmen Bauset Carbonell	Universidad Politécnica de Valencia Tesis doctoral	2012
The End of 'Corporate' Governance: Hello 'Platform' Governance	Mark Fenwick Joseph A. McCahery Erik P. M. Vermeulen	European Business Organization Law Review	2019
The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2016	Renee Murphy	Forrester Cambridge, USA	2016

Nota. Fuente: Universitat Politècnica de València, <https://riunet.upv.es/>

2.7. Crítica al estado del arte

Debido a la escasa información referente a los sistemas integrados de gestión de la Norma ISO/IEC 20000-1 para gestión de servicios de TI y la Norma ISO/IEC 27001 para la seguridad de la información, ha sido muy difícil obtener reseña de otros trabajos realizados que contengan una guía para la integración e implantación de las normas. La mayoría de resultados obtenidos en la búsqueda de información en el estado del arte no se encuentra información clara de una solución o modelo de integración de las normas ISO/IEC 27001 e ISO/IEC 20000.

En consecuencia, el desarrollo de este trabajo favorecerá y ayudará a futuras investigaciones relacionadas con este tema. Además, aportará una solución tecnológica efectiva que ayude en el desarrollo del análisis de deficiencias de las normas, ya que la implementación del software de GRC normalmente implica instalaciones complejas, sin embargo, las herramientas de análisis de

brechas o de deficiencias, permiten a los usuarios identificar la exposición al riesgo de la organización, para reunir en un informe la información y determinar las medidas a tomar.

Es importante vigilar los escenarios de riesgo en las empresas, para determinar la causa raíz de las amenazas y vulnerabilidades. Los riesgos son considerados altamente críticos en materia de la gestión de la seguridad de la información. En las empresas el tratamiento de los ataques y violaciones de seguridad debe contener una perspectiva reactiva y preventiva. Primero debe evaluarse y definirse el estado actual de la seguridad en las empresas para luego definir el estado futuro en base a las debilidades

El gobierno de las tecnologías y sistemas de información, conocido normalmente por gobierno de las TI (tecnologías de la información), es un tema cada vez más relevante para las empresas, ya que en ocasiones no se consigue un uso eficaz y eficiente de las TIC. En los últimos años han surgido numerosos marcos y normas que gozan del reconocimiento internacional, integrables con otros modelos de gestión, lo cual permite ir avanzando hacia una gestión integral en las organizaciones.

3. Análisis del Problema

Es importante el nivel de concienciación sobre amenazas y vulnerabilidades a todos los usuarios de las empresas, deben ser conscientes que las violaciones de seguridad y ciberdelincuencia son comunes y puede afectar a cualquier empresa, independientemente del tamaño y tipo de negocio. Las empresas deben evitar comportamiento y percepciones erróneas, tales como, que los criminales solo se interesan por las grandes empresas.

Por otra parte, el creciente interés de las empresas en mejorar sus procesos está llevando a que apuesten por implantar normativas que ayuden de forma estructurada el área de TI y la gestión de servicios TI, para mejorar la calidad y confiabilidad de TI en los negocios. Esta creciente adopción de estándares está generando nuevos desafíos en las organizaciones, debido a una serie de elementos:

- Por la necesidad de cumplir con las leyes y regulaciones relevantes.
- Optimizar el nivel de gastos de TI.
- Evaluar el desempeño para supervisar y mejorar las actividades de TI.
- El incremento de riesgos relacionados con TI.

El alcance para implementar las iniciativas de la seguridad de la información y la gestión de los servicios TI será diferente para cada empresa, por tanto, es necesario comprender el contexto y los factores específicos de los entornos internos y externos de la empresa. Las organizaciones necesitan administrar sus sistemas de gestión, haciéndolos compatibles, alineando los objetivos, teniendo una visión global de los sistemas y facilitando la toma de decisiones.

3.1. Identificación y análisis de soluciones posibles

Al implantar un sistema de gestión de la Norma ISO/IEC 27001 y la Norma ISO/IEC 20000, debemos tener claros los objetivos previsto para lograr una integración efectiva, y determinar el método de integración a aplicar. A continuación, se presentan un mapa de posibilidades para realizar la integración de los sistemas de gestión.

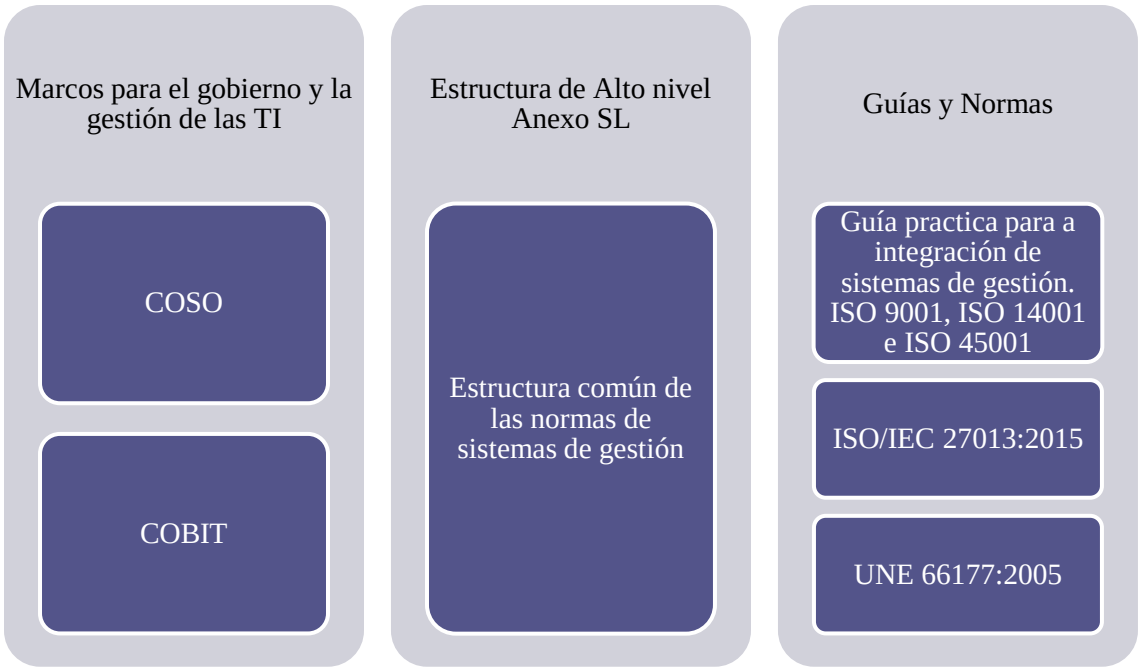


Figura 3. Mapa de posibilidades para la integración de sistemas de gestión

- Marcos de referencia de Gobierno TI.

  Consiste en utilizar marcos de Gobierno como COBIT 5, para proporcionar una serie de capacidades relacionadas con la seguridad de la información, tales como reducción de los incidentes de seguridad, una mejor toma de decisiones con conocimiento del riesgo y soporte para la fácil integración de estándares.

- Estructura de Alto nivel Anexo SL

  La utilización del Anexo SL, que define la nueva estructura de alto nivel para todos los estándares de sistemas de gestión, los términos y definiciones comunes. Facilita el manejo de sistemas de gestión integrados, proporcionando a las organizaciones la adopción de varios estándares de maneras más fácil.

- Guías y normas.

  Esta solución consiste en utilizar guías y normas para elaborar el plan de integración de las normas. Por ejemplo, la norma UNE 66177 está basada en el ciclo de mejora continua (o ciclo de Deming), donde establecen las directrices para desarrollar, implantar y evaluar un sistema integrado de gestión.

3.2. Análisis de requisitos de la aplicación web

A continuación, se detalla el caso de uso general y el diagrama de actividades de la herramienta.

Caso de uso general

Se muestra el diagrama de caso de uso que describe el comportamiento de la aplicación.

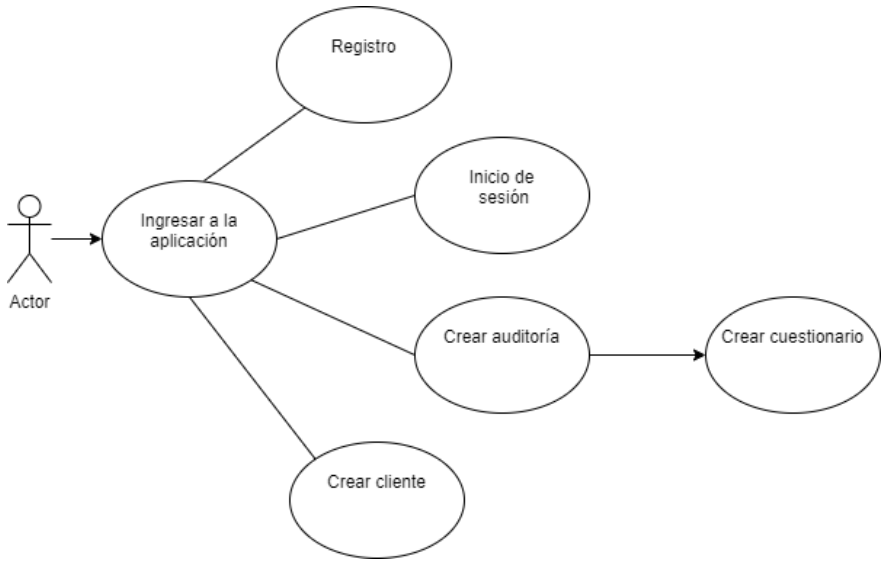


Figura 4. Diagrama de caso de uso general

Se muestra el diagrama de caso de uso que describe el comportamiento de la aplicación.

Tabla 3

Descripción casos de uso de aplicación web

Caso de uso:	Aplicación web para el análisis de deficiencias
Actor:	Usuario
Descripción:	El usuario se registra en la aplicación, para luego hacer inicio de sesión con el usuario y contraseña e ingresar a realizar el diagnostico
Actividades:	Registro de datos Inicio de sesión Crear cliente

- Rellenar datos
- Registrarse

Crear auditoría

- Seleccionar cliente
- Tipo de auditoría
- Fecha
- Contestar cuestionario

Nota. Elaboración propia

Diagrama de actividades

Se presenta el diagrama de actividades para mostrar el flujo de trabajo

- **Inicio de sesión en la herramienta**

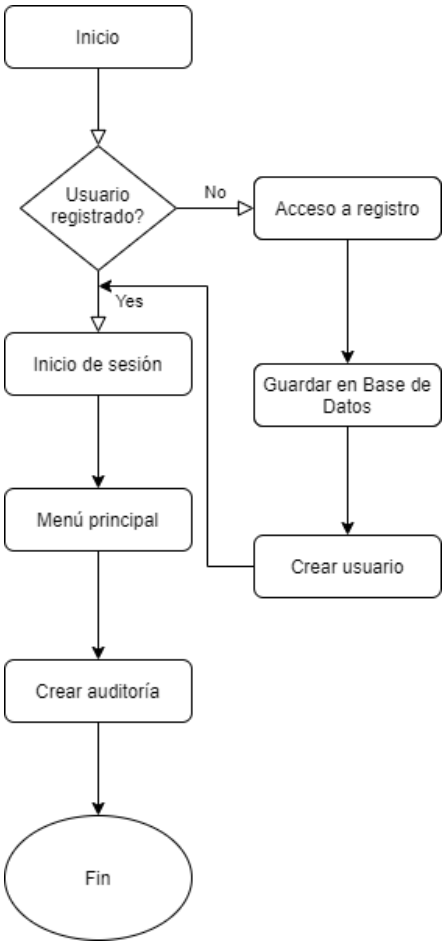


Figura 5. Diagrama de actividades de inicio sesión

- **Crear auditorías**

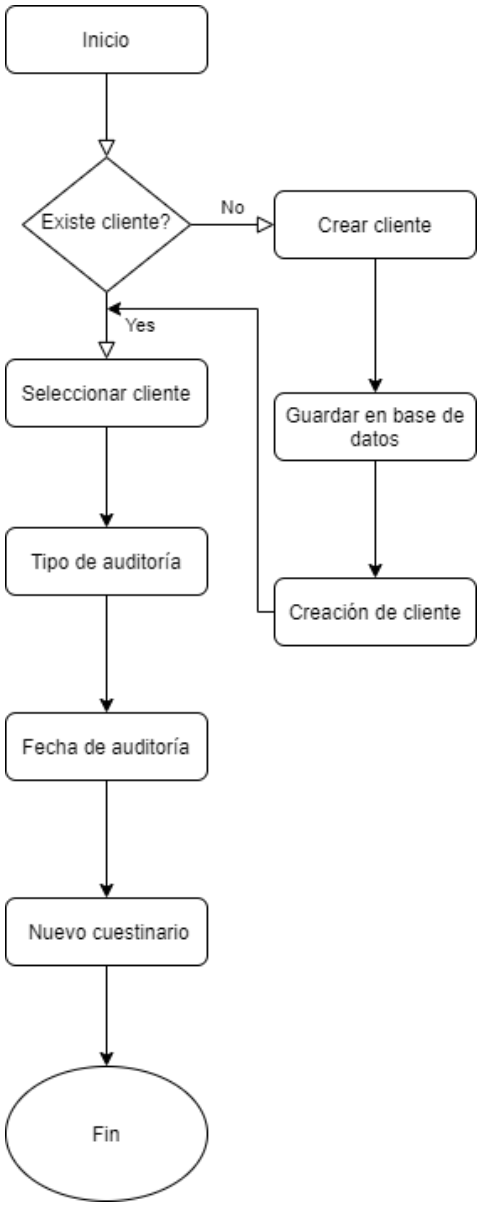


Figura 6. Diagrama de actividades crear auditorías

4. Solución propuesta

En el capítulo anterior se plantearon las posibles soluciones para realizar la implantación de las Normas ISO 27001 e ISO 20000 de forma integrada. El Modelo de implantación del Sistema Integrado de Gestión que se ha elegido, es la utilización de la norma ISO/IEC 27013, para eliminar la duplicidad innecesaria de procesos, teniendo en cuenta los siguientes enfoques de integración:

- Enfoque integrado para el establecimiento de los objetivos, la política de seguridad de la información y política de gestión de servicios TI.
- Enfoque integrado para la gestión de los riesgos
- Documentación integrada (manual de gestión, procedimientos, revisión por la dirección, etc.)
- Enfoque integrado de los procesos de mejora continua (acciones preventivas y correctivas)
- Enfoque integrado de las auditorías internas y externas.

Para el desarrollo del plan de integración se decidió utilizar la guía UNE 66177:2005 Sistemas de gestión, Guía para la integración de los sistemas de gestión. El proceso de integración de esta norma está basado en el ciclo de mejora continua.

El Modelo se implementa en función de las necesidades y requisitos específicos de la empresa y de sus objetivos de negocio, seleccionando los controles de seguridad adecuadamente para proteger los activos de la empresa y asegurar la confidencialidad a las partes interesadas.

El sistema de gestión integrado resultante de los requisitos específicos que describe la UNE 66177:2005, y el mapeo de los controles de la ISO/IEC 27013, se concentran los siguientes planteamientos a realizar en la implantación:

- Situación actual de la organización (evaluación de madurez de cada norma)
- Determinar el alcance
- Realizar el análisis de riesgo para conocer las amenazas y vulnerabilidades.
- Plan de tratamiento de riesgo
- Elaborar la política de seguridad y gestión de servicios TI.
- Plan de Implantación: ejecución progresiva de las tareas y actividades.

4.1. Mapeo de las normas ISO/IEC 27001 e ISO/IEC 20000

A continuación, se muestra la relación principal entre los controles de la norma ISO/IEC 27001 y los procesos de la norma ISO/IEC 20000.

Tabla 4

Correspondencia entre ISO/IEC 27001 e ISO/IEC 20000-1

ISO/IEC 27001	**ISO/IEC 20000-1**
4.3) Determinar el alcance del SGSI	4.3) Determinación del alcance del sistema de gestión de servicios
5) Liderazgo	5) Liderazgo
5.1) Liderazgo y compromiso	4.4) Sistema de gestión de servicios 5.1) Liderazgo y compromiso 6.1) Acciones para tratar riesgos y oportunidades 6.2.1) Establecer objetivos 7.3) Concienciación
5.2) Política	5.2) Política 7.3) Concienciación
5.3) Roles, responsabilidades y autoridades de la organización	5.3) Roles, responsabilidades y autoridades en la organización 7.4) Comunicación 4.2) Compresión de las necesidades y expectativas de las partes interesadas 8.1) Planificación y control operacional 8.2.2) Planificación de servicios 8.2.5) Gestión de activos
6.1.2) Evaluación de riesgos de seguridad de la información	6.1) Acciones para tratar riesgos y oportunidades 8.7.3.1) Política de seguridad de la información
7.1) Recursos	7.1) Recursos 7.2) Competencia

	7.3) Concienciación
7.3) Concienciación	7.2) Competencia 7.3) Concienciación
7.5) Documentación	7.5) Información documentada
7.5.1) Consideraciones generales	7.5.1) Generalidades 7.5.4) Información documentada del sistema de gestión de servicios
8.2) Análisis de riesgo	6.1) Acciones para tratar riesgos y oportunidades 8.7.3.1) Política de seguridad de la información
9.1) Monitorización, medición, análisis y evaluación.	9.1) Monitorización, medición, análisis y evaluación 9.2) Auditoría interna 9.3) Revisión por la dirección
9.2) Auditoría interna	9.2) Auditoría interna 10.1) No conformidad y acción correctiva
9.3) Revisión por Dirección	9.3) Revisión por la dirección
A.5.1) Políticas de seguridad de la información	6.1) Acciones para tratar riesgos y oportunidades 8.7.3.1) Política de seguridad de la información
A.12.3 Copias de seguridad	8.7.1) Gestión de la disponibilidad de servicios 8.7.2) Gestión de la continuidad de los servicios
A.15.1 Seguridad de la información en las relaciones con suministradores.	8.7.3.2) Controles de seguridad de la información
A.15.2 Gestión de la prestación del servicio por suministradores	8.2.3) Control de partes involucradas en el ciclo de vida de los servicios 8.1) Planificación y control operacional 8.3.1) Generalidades 8.3.4.1) Gestión de proveedores externos
A.16.1 Gestión de incidentes de seguridad de la	8.5.1.3) Actividades de gestión de

información y mejoras.	cambios 8.7.3.3) Incidencias de seguridad de la información
A.17.2 Redundancias	8.7.1) Gestión de la disponibilidad de servicios 8.7.2) Gestión de la continuidad de los servicios
A.18.1 Cumplimiento de los requisitos legales y contractuales	6.1) Acciones para tratar riesgos y oportunidades 8.7.3.1) Política de seguridad de la información
A.18.2 Revisiones de la seguridad de la información.	6.1) Acciones para tratar riesgos y oportunidades 8.7.3.1) Política de seguridad de la información 8.7.3.2) Controles de seguridad de la información 8.5.1.3) Actividades de gestión de cambios 8.7.3.3) Incidencias de seguridad de la información

Nota. Fuente: Adaptado de ISO/IEC (2015). Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. ISO/IEC 27013:2015. Switzerland

4.2. Ciclo de mejora continua o ciclo de Deming (PHVA)

Para implementar y gestionar el Sistema de Gestión Integrado de la norma ISO/IEC 27001 e ISO/IEC 20000-1, se utiliza el ciclo continuo PHVA (Planificar, Hacer, Chequear, Actuar).

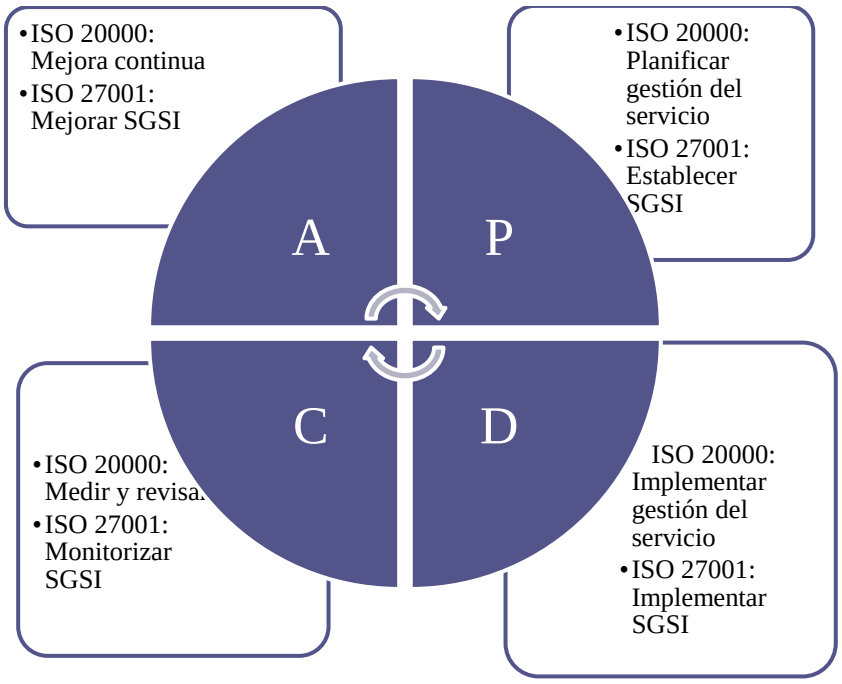


Figura 7. Ciclo de mejor continua

Tabla 5

Ciclo de mejora continua

FASE	**ACTIVIDAD**	**DOCUMENTO/REGISTRO**
Planificar	•Definir alcance: - Definir los límites del SGSI, se recomienda iniciar por un alcance limitado y justificar cualquier exclusión. - Definir el alcance del SGS •Definir política de seguridad y política de gestión de servicios:	Política, alcance y objetivos del SGSI y SGS. Procedimientos de soporte de SGSI y SGS Metodología de evaluación de riesgos Informe de evaluación de riesgos

	- La política incluye los objetivos de seguridad de la información de la organización y gestión de servicios, debe estar alineada con la gestión de riesgos y estar aprobada por la dirección. •Metodología de evaluación de riegos: definir el enfoque de evaluación de riesgos, es necesario delimitar una estrategia de aceptación de riesgo estableciendo los niveles de riesgo aceptable. •Inventario de activos: identificar todos los activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y el SGS. •Identificar amenazas y vulnerabilidad: identificar las amenazas relevantes asociadas a los activos y las vulnerabilidades que puedan ser aprovechadas por dichas amenazas. •Identificar impactos: identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo. •Análisis y evaluación de riesgos: evaluar la probabilidad de ocurrencia de un fallo de seguridad con relación a las amenazas y vulnerabilidades. Según los criterios de aceptación de riesgos determinar si el riesgo es aceptable o necesita ser tratado.	Declaración de aplicabilidad
Hacer	•Definir plan de tratamiento de riesgos: identificar las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.	Plan de tratamiento del riesgo Procedimientos específicos de operación del SGSI y SGS

	•Implantar plan de tratamiento de riesgos: alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades. •Formación y concienciación: proponer programas de formación en relación con la seguridad de la información a todo el personal. •Operar el SGSI: implantar normas, manuales procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad. •Operar el SGS: definir e implantar plan de gestión del servicio, procesos, registros, indicadores.	
Verificar	•Revisar el SGSI Y SGS: garantizar que el alcance definido sigue siendo el adecuado, detectar los errores en los resultados generados por el procesamiento de la información, prevenir eventos e incidentes de seguridad mediante indicadores. •Medir eficacia de los controles: verificar que se cumple con los requisitos de seguridad. •Revisar riesgos residuales: revisar y tener en cuenta los posibles cambios que hayan podido producirse en los objetivos y procesos de negocio, las amenazas identificadas y la efectividad de los controles implementados. •Realizar auditorías internas del SGSI y SGS: determinar si los controles, procesos y procedimientos del SGSI y SGS mantienen la conformidad con los requisitos de ISO 27001 e ISO 20000.	Informe de auditoría interna y de Revisión por la dirección
Actuar	•Implantar mejoras: comunicar las acciones y mejoras a las partes interesadas e implantarlas en el SGSI y el	Registros asociados

	SGS. •Acciones correctivas y preventivas: prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas •Comprobar eficacia de las acciones: asegurar que las mejoras introducidas alcanzan los objetivos previstos.	

Nota. Elaboración propia

4.3. Diseño de la aplicación web

A partir de las necesidades que se han conseguido de los casos de uso, se diseñan las pantallas de la aplicación que se pretende implementar.

Mockups

A la hora de diseñar la interfaz se utilizaron mockups para mostrar como quedará el diseño de la pagina web, y así generar una idea de como se verá el proyecto terminado.

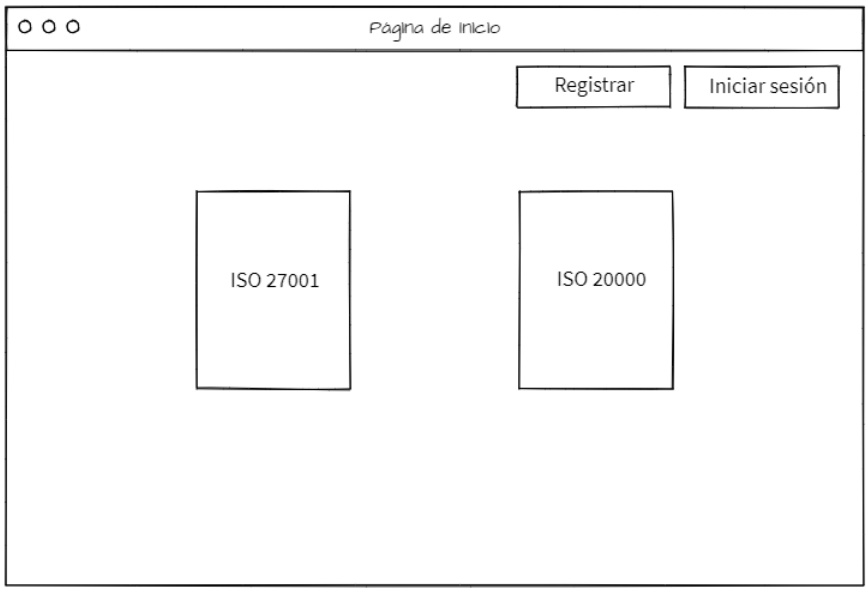


Figura 8. Estructura página de inicio

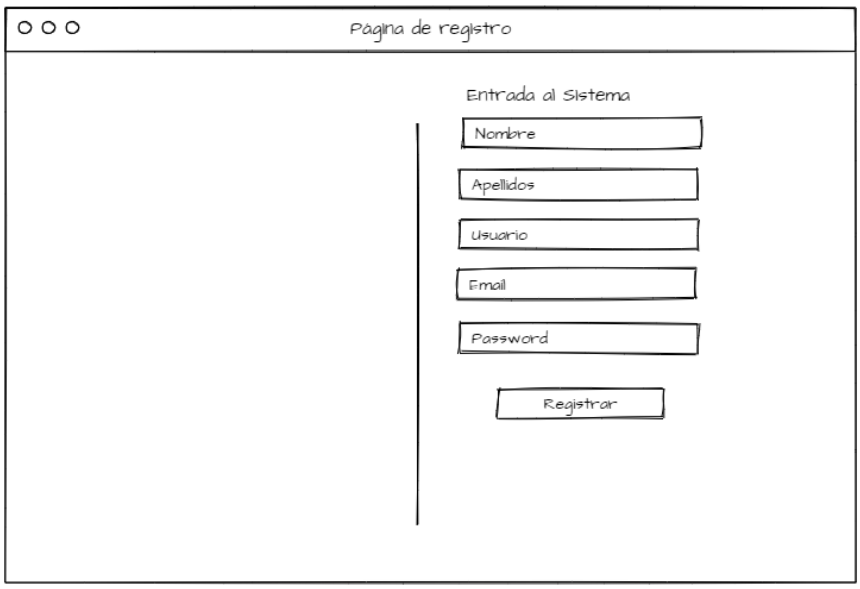


Figura 9. Estructura página de registro

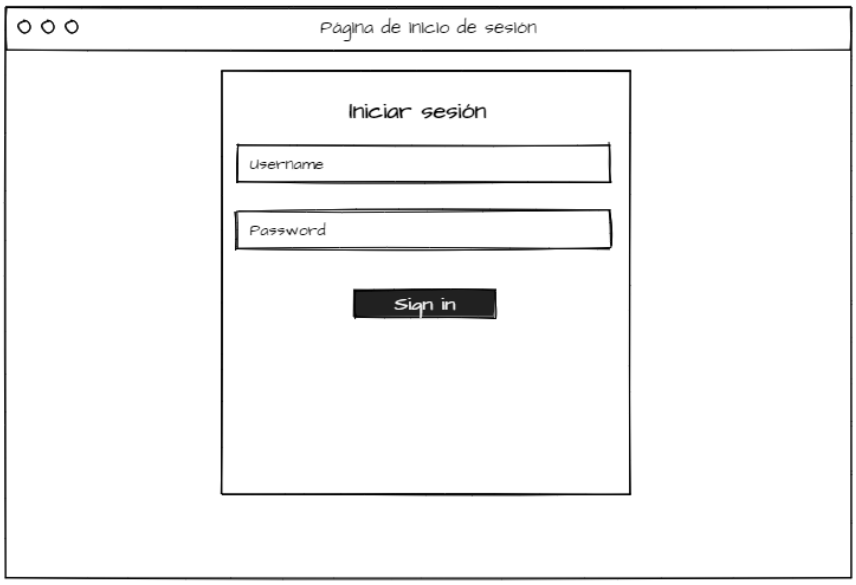


Figura 10. Estructura página inicio de sesión

Figura 11. Estructura registro de cliente

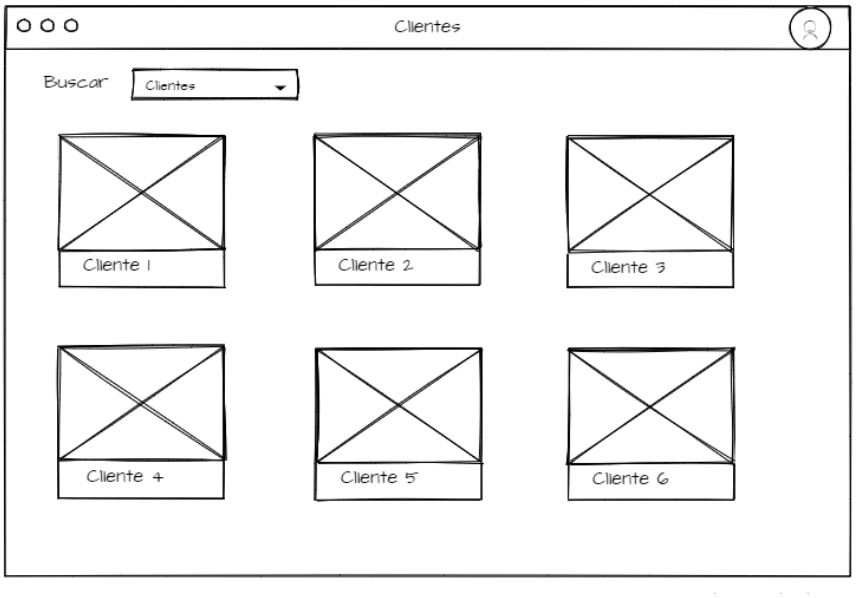


Figura 12. Estructura menú principal

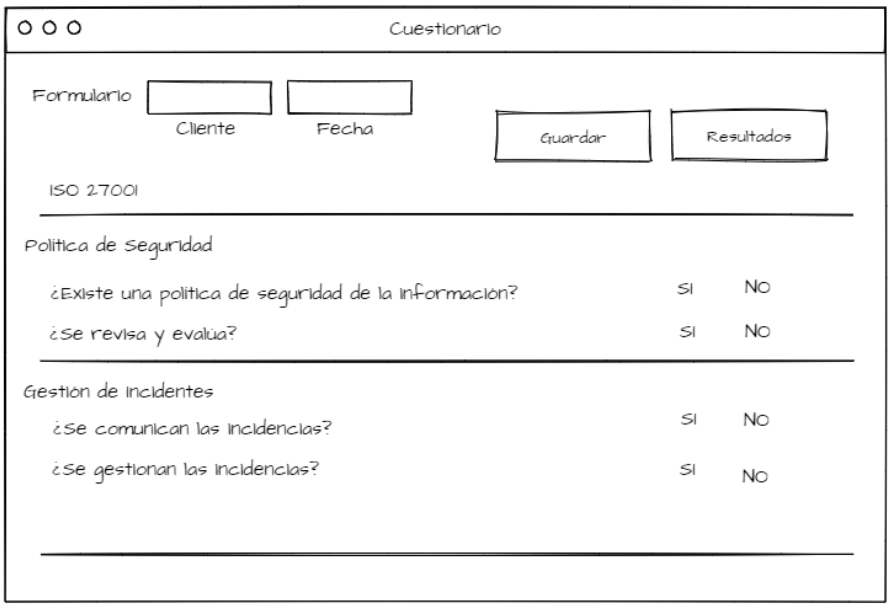


Figura 13. Estructura cuestionario de auditoría

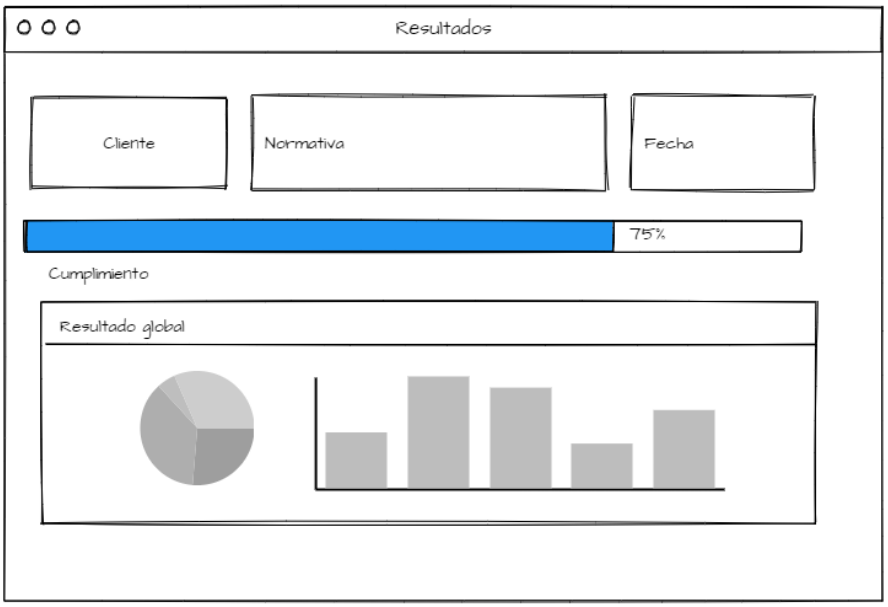


Figura 14. Estructura resultados de auditoría

Diagrama base de datos

La herramienta requiere de una base de datos que almacene toda la información, para el diseño se sigue el modelo relacional.

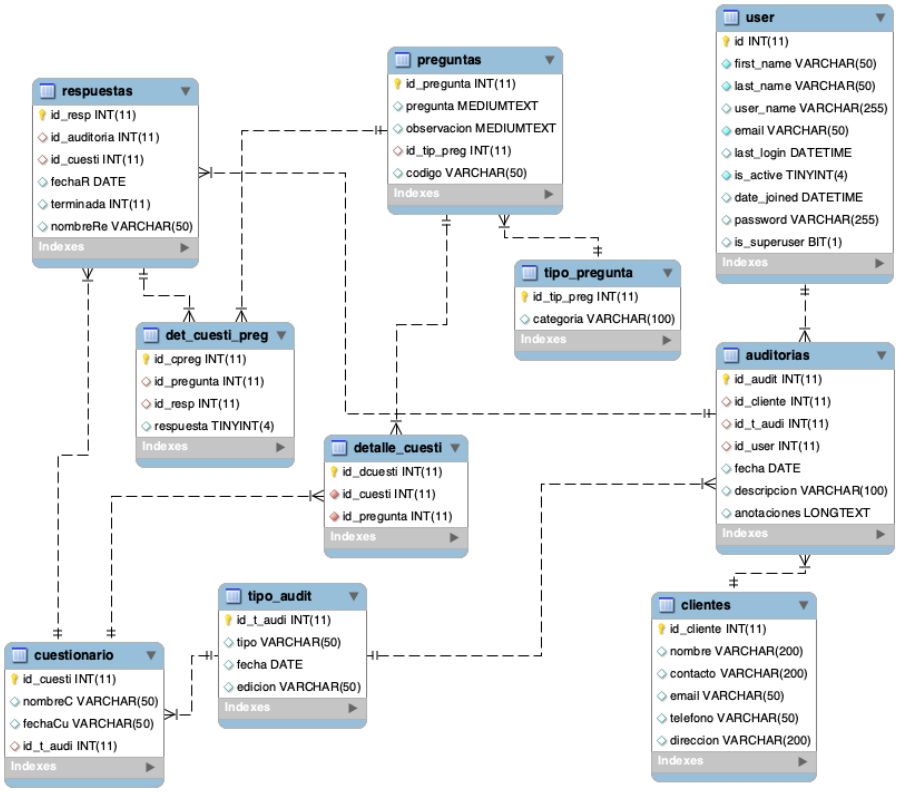


Figura 15. Diagrama E/R de la base de datos

- Tabla user: se almacena la información de los usuarios registrados que tengan acceso a la herramienta.
- Tablas auditorias: almacena la información general de las auditorías que crean los usuarios
- Tabla tipo_audit: el catálogo que contiene los tipos de auditorías que realiza la herramienta
- Tabla clientes: almacena la información relativa a los clientes que se les realiza la auditoría
- Tabla Cuestionario: registro general del cuestionario que pertenece a la auditoría
- Tabla detalle_cuesti: contiene las preguntas al cuestionario que va relacionado
- Tabla preguntas: catalogo que contiene las preguntas de las auditorías
- tipo_pregunta: contiene la categoría de las preguntas de cada normativa

- Tabla respuestas: contiene el registro general del resultado del cuestionario de la auditoría
- Tabla det_cuesti_preg: contiene el registro de respuesta de cada pregunta

Tecnología utilizada

Para realizar la parte práctica de la implementación de la aplicación web, se realizará mediante el uso de Node.js, como IDE de desarrollo Visual Studio Code, como lenguaje de programación JavaScript en la plataforma de Node.js, y como gestor de base de datos MySQL. Para las pruebas en local se utilizará XAMPP.

5. Implantación del Sistema de Gestión Integrado

Se analiza el modelo de Sistema Integrado de Gestión de las Norma ISO/IEC 27001 y la Norma ISO/IEC 20000-1, desarrollado en este trabajo. A partir de su aplicación en una empresa de servicios cloud, se muestran los resultados de los pasos a seguir obtenidos en la solución propuesta, para implantar las normas.

Pasos para la integración de los sistemas de gestión

- Situación actual de la organización (evaluación de madurez de cada norma)
- Determinar el alcance
- Realizar el análisis de riesgo para conocer las amenazas y vulnerabilidades.
- Plan de tratamiento de riesgo
- Elaborar la política de seguridad y gestión de servicios TI.
- Plan de Implantación: ejecución progresiva de las tareas y actividades.

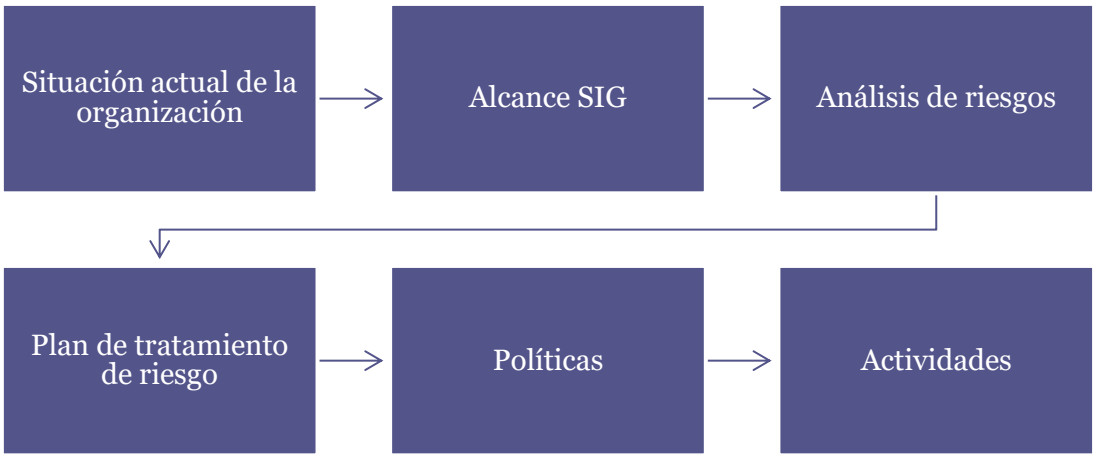


Figura 16. Diagrama de flujo de los pasos elementales para la integración de los sistemas de gestión

5.1. Presentación de la organización

VDC Data Center S.L. (en adelante VDC) es una empresa especializada en la implantación de soluciones Cloud. Se creó en 2013 y desde entonces ha tenido crecimientos exponenciales en clientes y soluciones tecnológicas en áreas como almacenamiento, virtualización e infraestructura cloud.

En la actualidad VDC está integrada por más de 70 profesionales, en su mayoría ingenieros informáticos y/o de telecomunicaciones, con una amplia experiencia en el sector TIC y atiende a más de 250 clientes tanto de la Comunidad Valenciana como del resto de España.

La misión es cubrir todas las necesidades tecnológicas de nuestros clientes en el ámbito de actuación escogido, con el objetivo prioritario de ser su catalizador para la mejora competitiva continua.

VDC presta a sus clientes los servicios de:

- Copias de seguridad en la nube. Nuestra solución es capaz de realizar copias de tus ordenadores, servidores físicos y entornos virtuales, en sistemas Windows y Linux. Una vez el software es instalado en tus sistemas, se empiezan a realizar las copias de seguridad a las que el administrador tendrá acceso, para gestionar las copias y realizar restauraciones, a través de una interfaz web

- El servicio contempla desde repositorios de copias de seguridad (backup) alojados en entorno completamente seguro y fiable, nuestro VDC Data Center S.L., hasta soluciones complejas de recuperación ante desastres, con opción de disponer de puestos de trabajo de emergencia en nuestras instalaciones.

- Virtualización de servidores. La virtualización de servidores permite un uso más eficiente de los recursos de TI que antes de la virtualización de servidores, era común tener hardware infrautilizado y sobre utilizado en el mismo centro de datos. Gracias a la virtualización, se pueden trasladar cargas de trabajo entre máquinas virtuales según su carga. El mismo servidor físico también puede ejecutar varios sistemas operativos y configuraciones de servidores, lo que incrementa aún más la eficiencia.

- Soporte y mantenimiento. Servicio de mantenimiento 24×7, nuestros especialistas están disponibles para ayudarle en cualquier problema que tenga con asistencia inmediata remota o presencial.

Organigrama general de la organización

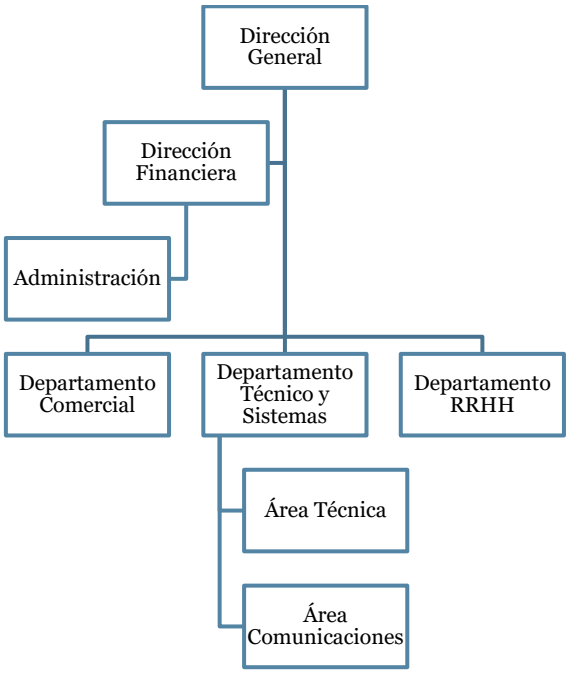


Figura 17. Organigrama de empresa

Necesidades de la organización

Los requerimientos de la seguridad de la información y los servicios de TI basados en los puntos débiles deben ser aceptados por la dirección como áreas que necesitan ser consideradas. Una vez obtenido el compromiso, es necesario contar con los recursos adecuados para apoyar la seguridad de la información y la gestión de los servidos TI.

Las necesidades de las partes interesadas de la organización se traducen a Metas de Empresas. Los puntos débiles relativos a la seguridad de la información proporcionan información sobre incidentes, problemas y riesgos detectados en VDC.

Con ayuda del mapeo entre las necesidades de las partes interesadas y las metas corporativas de COBIT 5 se obtienen las metas corporativas correspondientes.

Tabla 6

Mapeo metas corporativas y metas de Cobit

Puntos Débiles Más Comunes	Metas corporativas	Metas corporativas Cobit
La pérdida o robo de información causada por usuarios no autorizados que irrumpen en el sistema	Aumentar el nivel de seguridad	Riesgos de negocio gestionados (salvaguarda de activos)
Fallos en el cumplimiento de requerimientos legal, regulatorio o contractuales	Cumplir con la normativa de protección de datos	Cumplimiento de leyes y regulaciones externas
Denegación de servicio como resultado de ciberataques	Establecer los procesos y mecanismos necesarios para la prestación de los servicios	Continuidad y disponibilidad del servicio de negocio
Cambio tecnológico significativo o un nuevo paradigma	Establecer cuadros de mandos	Toma estratégica de Decisiones basada en Información
Recursos de TI insuficientes, personal con destrezas inadecuadas o personal insatisfecho laboralmente.	Definir roles y responsabilidades para cumplir con los servicios prestados	Optimización de costes de entrega del servicio
Fallos en el cumplimiento de las reglas de privacidad	Realizar formaciones en materia de seguridad a la organización	Cumplimiento con las políticas internas

Nota. Con ayuda del mapeo entre las necesidades de las partes interesadas y las metas corporativas de COBIT 5 se obtienen las metas corporativas correspondientes.

Tras la revisión inicial de los puntos débiles de la organización, se detectaron las siguientes deficiencias:

- VDC no tiene definida ni aplicada una política de seguridad de la información y gestión de servicios TI.
- No tienen establecidas unas directrices de seguridad de la información

- No han adoptado soluciones para mitigar la denegación de servicio
- Algunos empleados no tienen conocimiento suficiente para gestionar los servicios de forma adecuada.
- No se hace un uso completo de las herramientas disponibles para la gestión de VDC.
- No cumplen con las exigencias marcadas por la normativa vigente de protección de datos

Para dar solución a estas necesidades, la organización decide establecer un sistema de gestión integrado que cumpla con los requisitos de la Norma ISO/IEC 27001 e ISO/IEC 20000.

5.2. Aplicación del Sistema Integrado de Gestión

PASO 1. Evaluación de la madurez de la organización

En primer lugar, se realiza una evaluación inicial de la organización, para determinar el estado de cumplimiento de la norma ISO/IEC 27001 e ISO/IEC 20000. El resultado del análisis de madurez sirve como punto de referencia para establecer las soluciones y cumplir con los requisitos de cada una de las normas.

Para ello, se utiliza la herramienta web desarrollada donde se realiza el análisis de deficiencias. El Anexo IV presenta el manual de usuario de aplicación web.

Figura 18. Pantalla de inicio de la aplicación

Figura 19. Página principal de la aplicación

El Anexo V presenta un resumen de la evaluación de los dominios y resultado que muestra la aplicación. Una vez realizado el diagnóstico del análisis de deficiencia de las Normas ISO/IEC 27001 e ISO/IEC 20000, se presenta un resumen de los resultados y a continuación se destaca los más relevante.

Análisis de deficiencias de la Norma ISO/IEC 27001

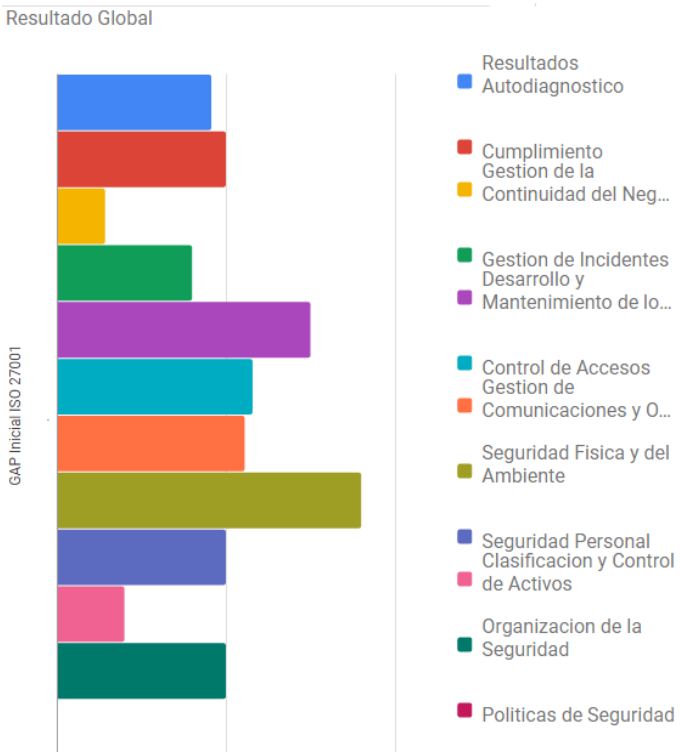


Figura 20. Ejemplo de los resultados del análisis de deficiencias de la Norma ISO/IEC 27001

- La entidad no dispone de un documento formal de Políticas de seguridad de la información. Es necesario que se documenten formalmente las políticas de seguridad, y

se comuniquen a todas las partes interesadas. Deberá asegurarse que las Políticas de Seguridad son revisadas, actualizadas y aceptadas por la Dirección.

- Todas las responsabilidades de la seguridad de la información deben estar definidas. Se debe crear la estructura organizacional oportuna a través de la cual tratar los aspectos relacionados con la seguridad de la información. Dirección debe alinear la seguridad de la información con los objetivos de negocio, para garantizar que la información de la organización está protegida adecuadamente.

- Se debe establecer un marco de gestión para controlar la seguridad de la información dentro de la organización. Los procedimientos de operación se deben documentar y revisar. La entidad no ha desarrollado documentos que dejen instrucción de cómo realizar las tareas de operación en los sistemas críticos

- Se debe asegurar que la información reciba un nivel de protección apropiado. Es necesario aplicar procedimientos para el manejo de la información aprobado por la organización.

- Se deben identificar todos los activos y elaborar un inventario, además se debe mantener y actualizar.

- La entidad no dispone de un plan de formación en materia de seguridad de la información. Todos los empleados de la organización deben recibir una adecuada capacitación en seguridad de la información.

- Se debe controlar los equipos de trabajo fuera del local de la organización. Es necesario determinar las directrices que la entidad marca sobre el uso de elementos de informática. Así como el desarrollo de procedimientos para las actividades de teletrabajo

- Se deben controlar los cambios en los medios y sistemas de procesamiento de la información. Es importante establecer procedimientos de apoyo a la operación de la seguridad, para el control de cambios mediante el uso de procedimientos formales.

- Se debe monitorizar el uso de los recursos y realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema, así como establecer un sistema de revisión de alertas de los sistemas monitorizados.

- Debe existir procedimientos para la gestión de los medios removibles. Los medios de almacenamiento que contienen información deben estar protegidos contra el acceso no autorizado.

- Es necesario disponer de un criterio adecuado de control de acceso. Debe existir un procedimiento formal para el registro de altas, bajas y modificación del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.

- Se debe requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de contraseñas. En la organización las contraseñas no caducan, se recomienda la configuración de cambio periódico de la contraseña al menos una vez al año

- Es necesario mantener un registro de toda la actividad para identificar posibles usos indebidos en el sistema. Es necesario mantener un adecuado registro con el fin de seguir la trazabilidad de las acciones de los usuarios del sistema

- Es necesario garantizar redundancia de los principales activos para garantizar la disponibilidad de los sistemas críticos.

- Se debe obtener la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando.

- Se debe asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información. Es necesario detectar problemas subyacentes indicados por repetición de incidentes de seguridad. También se debe establecer mecanismos para permitir cuantificar los tipos de los incidentes en la seguridad de la información.

- Es necesario definir los planes de contingencia para el riesgo más alto y de mayor impacto detectado. Los planes de continuidad del negocio deben ser probados y actualizados para asegurar que sean efectivos. El comité de crisis debe acelerar el proceso de toma de decisiones para solventar incidencias y/o crisis definiendo las prioridades, estableciendo la estrategia a seguir. Se debe mitigar el impacto financiero y

pérdida de información crítica ante incidentes. Es fundamental para la continuidad de los sistemas disponer de procedimientos formalmente establecidos al respecto. Se debe establecer la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos, mobiliario, infraestructuras físicas, etc.

- Se debe asegurar la protección y privacidad de datos conforme lo requiera la legislación.

- Los sistemas de información se deben revisar regularmente para ver el cumplimiento de los estándares de implementación de la seguridad. Se debe realizar una gestión de la mejora continua.

Análisis de deficiencias de la Norma ISO/IEC 20000

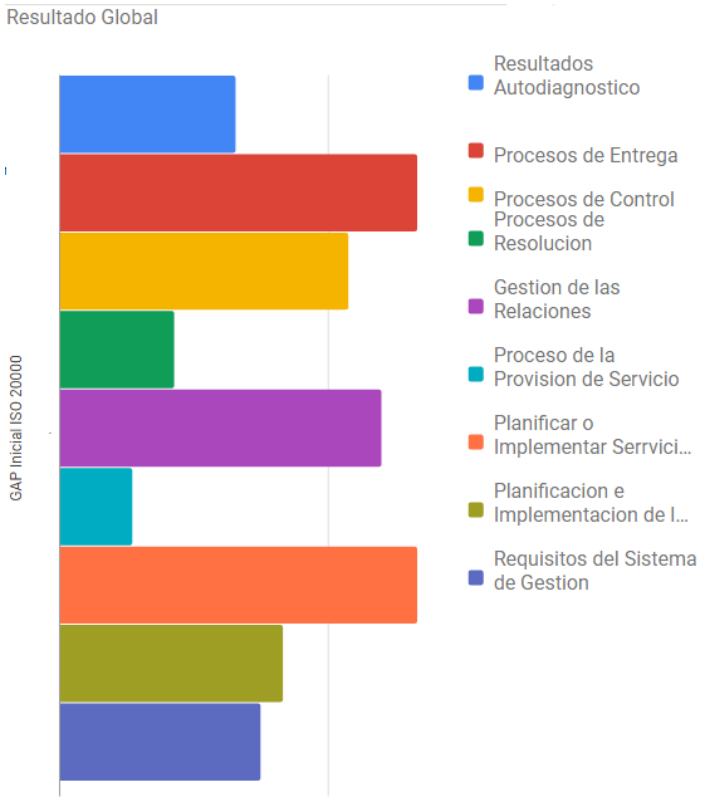


Figura 21. Ejemplo de los resultados del análisis de deficiencias de la Norma ISO/IEC 20000

- Se requiere la implementación de una serie de buenas prácticas, para obtener servicios bien planificados, diseñados, administrados y entregados. Debería existir un proceso para la creación y gestión de los documentos para ayudar a asegurar que se satisfacen las características descritas.

- Se debe establecer objetivos para la gestión del servicio. La política y planes de la gestión del servicio deben estar documentados.

- Se deben definir y mantener todos los roles y responsabilidades de la gestión del servicio, junto con las competencias que sean requeridas para su ejecución efectiva.

- Se debería conseguir los recursos necesarios y controlar el cumplimiento del presupuesto de la organización de TI.

- Se debe realizar un análisis de riesgos y determinar soluciones o medidas de protección a implementar.

- Es necesario realizar auditorías sobre la gestión del servicio, esta debe revisar el grado de implantación y funcionamiento del sistema de gestión del proveedor de servicios de TI.

- Dentro de los elementos que se deberían monitorizar, medir y revisar están la satisfacción del cliente, la utilización de los recursos y las tendencias. Las mejoras identificadas en los procesos deben ser remitidas al propietario del mismo, para registrarlas e incluirlas en el plan de mejora del servicio.

- La planificación de la gestión del servicio debería formar parte del proceso para convertir las necesidades de los clientes y las intenciones de los directivos en servicios y para proporcionar una guía para dirigir el progreso. El SLA detalla la particularización en la prestación de un servicio del catálogo a un cliente.

- Se deben detallar los contenidos, frecuencia y distribución de los informes. Los niveles de servicio se deben monitorizar y se deben generar informes, estos deben ser fiables, precisos y entregados a tiempo.

- Es necesario el desarrollo y actualización del plan de continuidad de TI, los planes de disponibilidad deben recoge las políticas, requisitos, directrices y toda la información necesaria para implementar y gestionar la disponibilidad de los servicios.

- Los incrementos de carga deben estar previstos, y los sistemas diseñados para absorberlos y también lo deben estar para poder crecer de forma dinámica. Es necesario

describir los niveles actuales de utilización de recursos y de rendimiento. Se debe realizar estimaciones sobre la capacidad necesaria en el futuro.

- La gestión de seguridad de la información es el proceso con responsabilidad sobre los niveles de seguridad de los activos utilizados para la prestación de los servicios de TI a los clientes. Se debe mantener un inventario de activos. En la evaluación de riesgos se realiza la identificación de los riesgos, y el análisis y valoración de los mismos. El proceso de gestión de la seguridad de la información también requiere que se traten los incidentes de seguridad.

- El tratamiento de las quejas es un instrumento esencial para la mejora del servicio. Se debe realizar un análisis de las encuestas, las quejas y las sugerencias del usuario.

- La gestión de los suministradores o proveedores debe garantizar la provisión sin interrupciones de los servicios de TI con calidad. La gestión de suministradores debe tener una actividad de revisión del propio proceso, analizando cómo está funcionando el proceso, si está siendo positivo para la organización, si se cumplen los objetivos definidos, etc.

- La gestión de incidencias es el proceso que se ocupa del tratamiento de los sucesos que provocan la degradación o pérdida del funcionamiento normal de un servicio, con el objetivo de recuperar el servicio para el cliente lo más rápidamente posible. Se debe priorizar la atención de incidencias de acuerdo con los compromisos de servicio. Se deben registrar todos los incidentes, para restaurar el servicio acordado con el negocio tan pronto como sea posible y responder eficientemente a las peticiones de servicio

- Todos los incidentes graves deberían tener en todo momento un gestor responsable claramente definido. La designación como responsable de un incidente debería proporcionar los niveles de autoridad para la función de coordinar y controlar todos los aspectos de la resolución. Un incidente mayor es uno que causa una interrupción grave de las actividades comerciales y debe resolverse con la mayor urgencia

- Se deben gestionar los problemas para evitar que se produzcan incidentes repetitivos o nuevos. Los problemas se pueden identificar a través de la aparición de varios incidentes que muestren síntomas comunes, por eso es importante realizar una clasificación de los mismos. El error conocido se trata como una unidad de información

específica y se debe registrar mediante una ficha que contiene el conocimiento sobre su resolución.

- Los informes de gestión de la configuración deberían estar disponibles para todas las partes correspondientes. Los procedimientos de auditoría de la configuración deben incluir el registro de deficiencias, el lanzamiento de acciones correctivas y la comunicación de su resultado.

- Se debe establecer un proceso responsable del control y tratamiento de los cambios en los servicios y en la infraestructura TI. Se debe asegurar que todos los cambios son registrados, evaluados, aprobados, implementados y revisados de una manera controlada.
- La gestión de entrega permite organizar y controlar los pasos al entorno de producción de los cambios aprobados. Se debería medir y analizar el número de incidentes relacionados con una entrega en el periodo inmediatamente posterior a un despliegue para evaluar su impacto en el negocio, en las operaciones y en los recursos de personal de apoyo

PASO 2. Determinar alcance

VDC Data Center S.L. establece un Sistema de Gestión Integrado, de acuerdo con los requisitos de las normas ISO/IEC 27001 e ISO/IEC 20000. Se ha propuesto como objetivo prioritario alcanzar la calidad y seguridad en los servicios que presta.

Para ello, se han definido unos compromisos de calidad y seguridad, definidos en la Política de seguridad de la información y gestión de servicios TI Integrada. Se han identificado los procesos de negocio de la organización.

- Procesos estratégicos: vinculados al ámbito de las responsabilidades de la dirección.
- Procesos clave: son los procesos ligados a la prestación del servicio.
- Procesos de soporte: son aquellos que dan soporte a los procesos claves.

Se determina el alcance para ISO/IEC 27001:2013

Sistemas de Información que dan soporte a los servicios de VDC Data Center S.L. según Declaración de Aplicabilidad en su versión vigente.

Se determina el alcance para ISO/IEC 20000-1:2018

Sistema de Gestión del servicio cloud de VDC Data Center S.L.

PASO 3. Análisis de riesgos

Debemos identificar los activos más importantes que guardan relación con el departamento de sistemas de la organización, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Para identificar las amenazas se utiliza el catalogo de amenazas de la metodología MAGERIT v3.

Por último, medimos el nivel de riesgos de lo que puede ocurrir y se valora. Para cada activo, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría.

Para el cálculo de la de probabilidad tenemos según escala de tres valores.

Tabla 7

Estimar la probabilidad

VALOR	DESCRIPCIÓN
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Nota. Fuente: INCIBE Protege tu empresa - blog (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

Para el cálculo del impacto tenemos según escala de tres valores.

Tabla 8

Estimar el impacto

VALOR	DESCRIPCIÓN
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Nota. Fuente: INCIBE Protege tu empresa - blog (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

Se establecen los siguientes criterios para determinar la aceptación del riesgo por parte de la organización.

Tabla 9

Criterios de aceptación del riesgo

RANGO	**DESCRIPCIÓN**
Riesgo <= 9	La organización considera el riesgo poco reseñable.
Riesgo > 9	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Nota. Fuente: INCIBE Protege tu empresa - blog (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

Para calcular el riesgo se utiliza la siguiente matriz

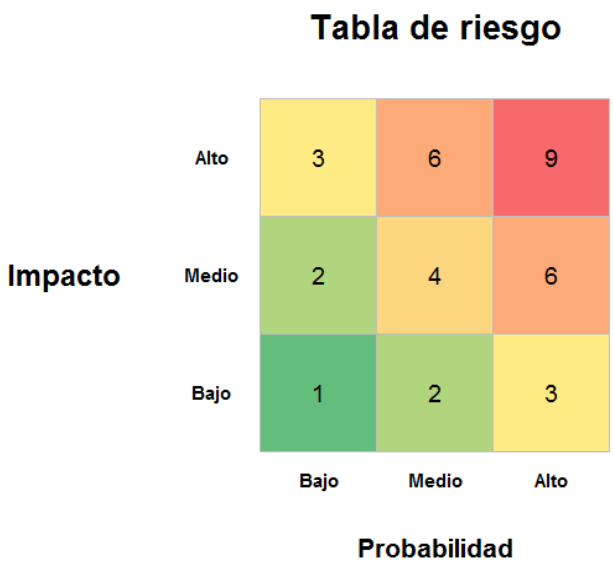


Figura 22. Matriz de riesgos
Nota. Fuente: INCIBE Protege tu empresa - blog (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

Se deben tratar aquellos riesgos que superen el límite establecido. Trataremos aquellos riesgos cuyo valor sea superior a “9”.

Tabla 10

Análisis de riesgos

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
HARDWARE				
HW1-EQUIPOS	Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
HW2-EQUIPOS	Abuso de privilegio de accesos	3	3	9
HW1-SERVIDORES	Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
HW1-CABINA DE DISCOS	Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
HW-IMPRESORAS	Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
HW-CABINA BACKUP	Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
HW-PORTATIL	Errores de mantenimiento / actualización de equipos (hardware)	1	3	3
HW-TELÉFONO	Errores de mantenimiento / actualización de equipos (hardware)	1	3	3

MAQUINAS VIRTUALES				
HWV-SERVIDOR DNS	Errores de mantenimiento / actualización de programas (software)	2	3	6
HWV-SERVIDOR DOMINIO	Errores de mantenimiento / actualización de programas (software)	2	3	6
HWV-SERVIDOR DE FICHEROS	Errores de mantenimiento / actualización de programas (software)	2	3	6
HWV1-GESTOR DOCUMENTAL	Errores de mantenimiento / actualización de programas (software)	1	2	2
HWV-SERVIDOR DHCP	Errores de mantenimiento / actualización de programas (software)	1	2	2
HWV1-CORTAFUEGOS	Errores de mantenimiento / actualización de programas (software)	2	3	6
COMUNICACIONES				
COM-COMUNICACIONES DATA CENTER	Caída de sistema por sobrecarga	1	2	2
COM-FIREWALL	Caída de sistema por sobrecarga	1	2	2
COM-AREA LOCAL	Caída de sistema por sobrecarga	1	3	3
COM-WIFI	Caída de sistema por sobrecarga	1	2	2
COM-RADIOENLACE	Caída de sistema por sobrecarga	1	2	2

COM-ROUTER	Caída de sistema por sobrecarga	1	2	2
APLICACIONES				
SW-TEAMS EMPRESARIAL	Errores de mantenimiento / actualización de programas (software)	2	3	6
SW-APLICACIONES OFIMATICAS	Errores de mantenimiento / actualización de programas (software)	2	3	6
SW-APLICACIONES DE GESTIÓN	Errores de mantenimiento / actualización de programas (software)	2	3	6
SW-APLICACIONES DE SISTEMAS	Errores de mantenimiento / actualización de programas (software)	2	2	4
SERVICIOS SUBCONTRATADOS				
SS-PROVEEDOR DE DATOS	Interrupción de otros servicios y suministros esenciales	1	3	3
SS-OFFICE 365	Interrupción de otros servicios y suministros esenciales	2	2	4
SS-PROVEEDOR LINEA DE VOZ	Interrupción de otros servicios y suministros esenciales	1	3	3
ELEMENTOS AUXILIARES				
AUX-CLIMATIZACIÓN	Condiciones inadecuadas de temperatura o humedad	1	3	3
AUX-SUMINISTRO ELECTRICO	Corte del suministro eléctrico	2	2	4

DATOS				
D-CLIENTES	Fuga de información	1	3	3
D-SLA	Corrupción de la información	2	2	4
D-CONEXIÓN CLIENTE	Acceso no autorizado	1	3	3
INSTALACIONES				
L-CPD	Daños por agua	1	3	3
L-OFICINAS	Fuego	2	2	4
PERSONAL				
P-ADMINISTRATIVO	Ingeniería social	3	3	9
P-TECNICO	Indisponibilidad del personal	2	2	4
SERVICIOS				
S1-SERVICIOS DATA CENTER	Errores de los usuarios	1	3	3
S2-SERVICIOS DATA CENTER	Errores del administrador	1	3	3

Nota. Fuente: INCIBE Protege tu empresa (2015) - ¿Qué te interesa? Plan director de seguridad. <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad>

PASO 4. Tratamiento del riesgo

Una vez establecido el criterio de aceptación de los riesgos, quedarán determinados por tanto los riesgos no aceptables por la empresa VDC Data Center S.L., y éstos deberán ser tratados según cada caso con las medidas correspondientes.

A partir de los resultados de la evaluación de riesgos y del umbral de riesgo definido, la dirección determinará las acciones pertinentes en cada caso.

Tabla 11

Tratamiento del riesgo

Activo	Amenaza	Riesgo	Plan de acción
HW1-EQUIPOS	Errores de mantenimiento / actualización de equipos (hardware)	9	Establecer una periodicidad para llevar a cabo las tareas preventivas que garanticen el buen funcionamiento de los equipos
HW2-EQUIPOS	Abuso de privilegio de accesos	9	Eliminar privilegios de administrador para los usuarios administrativos en los equipos
HW1-SERVIDORES	Errores de mantenimiento / actualización de equipos (hardware)	9	Ejecutar análisis de vulnerabilidades técnicas de forma periódica
P-ADMINISTRATIVO	Ingeniería social	9	Realizar formación al personal sobre estrategias de seguridad de la información (uso correcto del correo electrónico, claves de seguridad, etc.)

Nota. Elaboración propia

PASO 5. Política de seguridad de la información y gestión de servicios TI

VDC Data Center S.L. es una empresa especializada en la implantación de soluciones Cloud. Se creó en 2013 y desde entonces ha tenido crecimientos exponenciales en clientes y soluciones tecnológicas en áreas como almacenamiento, virtualización e infraestructura cloud.

Áreas de negocio:

- Soluciones TIC: Data Center
- Servicios: Copias de seguridad en la nube, Virtualización de servidores, Soporte y mantenimiento.

Esta política se establece como marco en el que se deben desarrollar todas las actividades de la empresa de manera que se garantice a los clientes y demás partes interesadas.

En consecuencia, el empleado se compromete a:

- Preservar la seguridad y confidencialidad de la información, de sus clientes y proveedores.
- Actuar con buena fe y con la debida diligencia en orden a su condición de empleado.
- Utilizar y emplear los datos exclusivamente para el fin para los que le fueron suministrados.
- Abstenerse de sacar información relevante o no, si no es con el previo y preceptivo consentimiento de la organización.
- No podrá desarrollar actividad con empresas consideradas de la competencia, sin contar con el previo y por escrito consentimiento de la organización.
- Cesar en la prestación de cualquier actividad ilícita o perjudicial para la organización
- Abstenerse bien en su propio nombre o por cuenta de cualquier otra persona, firma o sociedad, a facilitar información considerada como confidencial en cualquier momento inmediatamente posterior a la fecha del cese, dimisión o abandono de la empresa.

Se establece una serie de directrices en torno a las actividades de gestión de los servicios TI desarrolladas por la organización. Estas directrices son:

- Se establecerán niveles de servicio por defecto para cada para cada uno de los servicios provistos por la organización. Todo el personal velará porque los servicios prestados cumplan con dichos acuerdos de nivel de servicio.

- Todos los servicios TI proporcionados deberán estar adecuadamente monitorizados Todo el personal participará en la identificación de los requerimientos de disponibilidad y continuidad de los servicios TI proporcionados por la organización.
- Todos los servicios TI prestados por la organización estarán adecuadamente presupuestados, considerando tanto los costes directos como los indirectos
- Todo el personal implicado en la prestación de servicios TI cuidará de que los servicios ofrecidos satisfagan las demandas de servicio de sus respectivos usuarios.

Se analizarán los riesgos de seguridad de la información de todos los servicios TI prestados por la organización, y se establecerán los controles asociados necesarios para mitigar los riesgos identificados.

La presente política es conocida y suscrita por todo el personal de VDC DATA CENTER S.L. conforme a las exigencias de la dirección.

PASO 6. Plan de actividades para implantación

El plan de implantación consta de una serie de tareas y actividades destinadas a subsanar las insuficiencias detectadas en la evaluación de madurez de la organización.

ACTIVIDAD	INICIO DEL PLAN	DURACIÓN DEL PLAN	INICIO REAL	DURACIÓN REAL	PORCENTAJE COMPLETADO
Determinar alcance	1	4	1	2	100%
Crear Comité	1	2	1	4	50%
Roles y responsabilidades	2	2	2	3	35%
Establecer objetivos	4	4	4	6	10%
Políticas	4	2	4	6	85%
Análisis de riesgos	4	6	4	6	100%
Manual de gestión	5	4	5	6	50%
Clasificación de Información	5	2	5	5	60%
Directrices de seguridad y teletrabajo	5	2	5	6	75%
Instrucciones de operación	6	5	6	7	50%
Necesidades formación	6	1	5	8	60%
Gestión de vulnerabilidades	7	3	8	3	0%
Continuidad del negocio	7	6	8	7	50%
Presupuestos servicio	7	3	8	1	0%
Satisfacción del cliente	7	4	8	5	1%
Tratamiento encuentas	8	5	10	3	80%
Gestión de cambios	9	2	10	5	0%
Gestión de problemas	9	6	10	7	0%
Gestión de incidencias	9	1	10	5	0%
Auditoría CMDB	10	5	11	6	0%
Auditorías internas	11	8	11	2	0%
Revisión por la dirección	11	7	11	3	0%
Certificación de las normas	12	1	12	2	0%

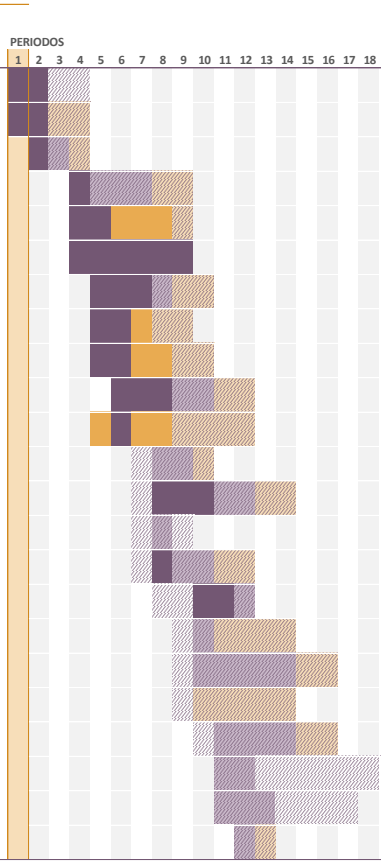


Figura 23. Actividades para la implantación del sistema integrado de gestión

6. Conclusiones

En este Trabajo de Fin de Máster (TFM), se ha ofrecido una visión de la Norma ISO/IEC 27013:2015 para identificar los procesos comunes de las Normas ISO/IEC 27001:2013 e ISO/IEC 20000-1:2018 y presentar un modelo de sistema integrado de gestión con un enfoque compartido de la organización, para mejorar la eficacia y rentabilidad del negocio.

Para desarrollar la implantación del sistema integrado de gestión se han acometido una serie de acciones, que se mencionan a continuación:

- Se han analizado los procesos de gestión de servicios de TI de la Norma ISO/IEC 20000 y los controles de seguridad de la información de la Norma ISO/IEC 27001. A partir de este análisis se ha elaborado un mapa de relaciones entre los controles de las normas.
- Se ha desarrollado la herramienta informática para diagnosticar el nivel de madurez de los procesos de gestión de servicios de TI y los controles de seguridad de la información.
- Finalmente se ha validado el desarrollo de la aplicación web para el análisis de deficiencias en una empresa de servicios cloud, obteniendo el resultado para ejecutar las acciones de mejora propuestas por cada una de las normativas.

El desarrollo de esta herramienta concede a los auditores, consultores y empresas llevar a cabo las tareas de revisión del cumplimiento de los requisitos del Sistema de Gestión, respecto a la norma pertinente de forma conjunta, debido a que en la actualidad no hay aplicaciones que permitan ejecutar el trabajo de manera integrada de las diferentes normas, aportando importantes ventajas para el negocio como puede ser ahorro de costes y tiempo de ejecución.

Además, la herramienta facilita la gestión de forma centralizada de las insuficiencias detectadas, para poner en marcha el plan de actividades que proporciona las bases de la implantación. También mejora el análisis y la interpretación de los resultados obtenidos del modelo de evaluación, presentando en formato gráfico el nivel de madurez de cada proceso.

Según los objetivos planteados en este trabajo, se presentan los principales beneficios que tienen las empresas al contar con un sistema integrado de gestión:

- Mejorar la imagen corporativa y la confianza del cliente
- Lograr posición en el mercado frente a la competencia.
- Menor coste de implantación de dos proyectos.

- Reducción del tiempo por la integración de los procesos comunes
- Eliminación de duplicidades de procedimientos e instrucciones.
- Distribución de los esfuerzos y recursos necesarios
- Concienciar a todas las partes interesadas de la organización, sobre los servicios proporcionados y la seguridad de los sistemas de información.
- Realizar auditorías integradas

Relación TFM con estudios cursados

Durante la realización del master dos de las materias que constituyen el programa formativo son la “Gestión y Gobierno de las TI” y “Administración electrónica”, estas asignaturas despertaron mi interés en los temas relativos al gobierno y gestión de las TI, y mi desarrollo profesional en consultoría de seguridad.

Las competencias trasversales son:

- Innovación, creatividad y emprendimiento. Proceso de la búsqueda de oportunidades de mejora, generación de ideas y llevar una implementación a través de un plan de acción.
- Comunicación efectiva. Presentación del trabajo a desarrollar.

Trabajo futuro

A continuación, se exponen las líneas de investigación futuras que podrían dar continuidad a este trabajo y que sirven para mejorar el desarrollo tecnológico realizado:

- En primer lugar, se plantea generar reportes en formato PDF.
- Otra posibilidad de ampliación de la herramienta sería desarrollar un análisis comparativo del resultado de los informes.
- Por último, añadir un módulo de roles de usuarios, para agregar un usuario administrador que realice las modificaciones a nivel del sistema.

7. Referencias

[1] AENOR (2005). *Sistemas de gestión. Guía para la integración de los sistemas de gestión.* UNE 66177:2005. Madrid: AENOR

[2] AENOR (2014). *Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información.* ISO/IEC 27001:2013. Madrid: AENOR

[3] Amutio, M., Candau, J., & Mañas, J. (2012). MAGERIT–*versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I-Método*. Madrid. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>

[4] CCN (2020). *IA-13/20 Ciberamenazas y Tendencias. Edición 2020* <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html>

[5] CCN (2019). *IA-13/19 Ciberamenazas y Tendencias. Edición 2019* <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html>

[6] CCN (2018). *Guía de Seguridad de las TIC. CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes* <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html>

[7] FERNÁNDEZ SÁNCHEZ, C. M. y PIATTINNI VELTHUIS, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* Madrid: AENOR.

[8] Fenwick, M., McCahery, J. A., & Vermeulen, E. P. (2019). *The end of 'corporate'governance: hello 'platform'governance. European Business* Organization Law Review, 20(1), 171-199.

[9] Haro, E., Guarda, T., Peñaherrera, A. O. Z., & Quiña, G. N. (2019). *Desarrollo backend para aplicaciones web, Servicios Web Restful: Node. js vs Spring Boot*. Revista Ibérica de Sistemas e Tecnologias de Informação, (E17), 309-321.

[10] INCIBE *Protege tu empresa - Guías (2015). Gestión de riesgos. Una guía de aproximación para el empresario.* <https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario>

[11] INCIBE *Protege tu empresa (2015) - ¿Qué te interesa? Plan director de seguridad.* <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad>

[12] INCIBE *Protege tu empresa - blog (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos.* <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>

[13] ISMS FORUM SPAIN. *Asociación española para el fomento de la seguridad de la información* < https://www.ismsforum.es>

[13] Isaca, C. (2012). 5: *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Rolling Meadows.

[14] Isaca, (2013). *Transformando la ciberseguridad*. Rolling Meadows.

[16] ISO27000.ES. *Portal para la norma ISO 27001 en español* < https://www.iso27000.es>

[17] ISO/IEC (2015). *Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. ISO/IEC 27013:2015*. Switzerland

[18] Luján-Mora, S. (2002). *Programación de aplicaciones web: historia, principios básicos y clientes web*. Editorial Club Universitario.

[19] Murphy, R. (2016). *The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2016*. Cambridge, USA.

[20] Node, J. S. *Acerca de Node. js®. Node. js Foundation* < https://nodejs.org/es/about>

[21] Telefónica, S. A. (2010). ISO/IEC 20000. *Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. España: AENOR.

[22] UNE (2018). *Tecnologías de la información. Gestión de Servicios. Parte 1: Requisitos del Sistema de Gestión de Servicios.* ISO/IEC 20000-1:2018. Madrid: AENOR

[23] Valarezo Pardo, M., Honores Tapia, J., Gómez Moreno, A., & Vinces Sánchez, L. (2018). *COMPARACIÓN DE TENDENCIAS TECNOLÓGICAS EN APLICACIONES WEB. 3C Tecnología. Glosas De Innovación Aplicadas a La Pyme*, 28-49. Recuperado a partir de <http://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/618>

[24] Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T. (2008). *Fundamentos de ITIL® (Vol. 3)*. Van Haren.

[25] Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T. (2008). *Estrategia del Servicio basada en ITIL® (Vol. 3).* Van Haren.

[26] Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Verheijen, T. (2008). *Diseño del Servicio basada en ITIL® (Vol. 3).* Van Haren

Anexos

Anexo I. Resumen de la Norma ISO/IEC 27001

Sistema de Gestión de la Seguridad de la Información (SGSI)

La definición de Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001:2013 es:

> *Un sistema de gestión para la Seguridad de la información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que afectan a la seguridad de la información en una empresa u organización.*

ISO 27001 es una norma internacional que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. La gestión de la seguridad debe realizarse mediante un proceso sistemático y conocido por toda la organización. La Confidencialidad, Integridad y Disponibilidad son tres términos fundamentales de la seguridad de la información.

- Confidencialidad: es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Integridad: es la propiedad de la información relativa a su exactitud y completitud.
- Disponibilidad: es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

El alcance y los límites del SGSI deben definirse en términos de la actividad empresarial, de la organización, su ubicación, sus activos y tecnología.

Contexto de la organización

Conocer la organización y su contexto se plantea como un requisito inicial para poder establecer un punto de referencia en la aplicación del sistema de gestión de la seguridad de la información.

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.

Liderazgo

Los requisitos relacionados con el liderazgo se refieren al compromiso que debe ejercer la dirección de la empresa en el proceso de implantación de un SGSI.

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información:

- asegurando que se establecen la política y los objetivos de seguridad de la información
- asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles
- promoviendo la mejora continua

La política del SGSI

La política del SGSI debe recoger y transmitir el compromiso de la dirección que proporcione las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran llevar a cabo para la gestión de seguridad en la organización.

La política de seguridad de la información debe considerarse como una declaración de alto nivel y debe describirse claramente los enlaces a otras políticas específicas como:

a) Política de control de acceso: proporciona un uso adecuado a las partes interesadas.
b) Política de seguridad física y ambiental: protección de ubicaciones físicas y controles ambientales que proporcionen capacidad a las operaciones de soporte.
c) Política de gestión de incidentes: responder a los incidentes de una manera oportuna para recuperar las actividades de negocio.
d) Política de continuidad de negocio: análisis de impacto en el negocio, planes de contingencia de negocio y plan de recuperación de desastres.
e) Política de gestión de activos: clasificación y propiedad de la información, de los sistemas.
f) Política de gestión de riesgos: plan de gestión del riesgo corporativo
g) Política de gestión de proveedores: gestión de los contratos (términos y condiciones).

Planificación

Tras identificar las necesidades y expectativas de las partes interesadas, es importante establecer un plan para definir los riesgos a tratar y las actividades a realizar para mitigar dichos riesgos.

- La organización debe definir y aplicar un proceso de apreciación de riesgos de seguridad de la información
- La organización debe definir y efectuar un proceso de tratamiento de riesgos de seguridad de la información
- La organización debe establecer los objetivos de seguridad de la información.

Soporte

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

- Gestión de los recursos
- Competencia y concienciación del personal
- Comunicación y concienciación de todas las de todas las partes interesadas

Operación

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información. Cuando se aceptan riesgos debe quedar evidencia, como las firmas de los propietarios de activos que lo reconocen formalmente aceptando así la responsabilidad por cualquier incidente que surja.

Evaluación del desempeño

Es importante evaluar el desempeño de las acciones emprendidas.

- La organización debe llevar a cabo auditorías internas del sistema de gestión de seguridad de la información.
- La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización.

Mejora

Las no conformidades son requisitos del SGSI parcial o totalmente insatisfechos, pueden documentarse en forma de problemas, eventos, incidentes, hallazgos de auditoría y revisión, etc. Es necesario mantener un registro de no conformidades, junto con la evidencia de las acciones emprendidas.

La organización debe mejorar de manera continua la eficacia del sistema de gestión de seguridad de la información.

Anexo II. Resumen de la Norma ISO/IEC 20000

Sistema de Gestión del Servicio (SGS)

El término "sistema de gestión", representa una manera formalizada de realizar las cosas. Así, el sistema de gestión del servicio (SGS) es una forma normalizada de gestionar los trabajos necesarios para crear y mantener plenamente utilizables los servicios.

Un Sistema de Gestión de Servicios presta soporte a la gestión del ciclo de vida de los servicios, incluyendo la planificación, el diseño, la transición, la entrega y la mejora de los servicios, que cumplen con los requisitos acordados y ofrecen valor para los clientes, los usuarios y la organización que presta los servicios.

La norma ISO/IEC 20000 define los procesos y actividades esenciales para que las áreas de TI puedan prestar un servicio eficiente y alineado con las necesidades de la empresa. Esta norma construida sobre sobre la base del modelo ITIL, se centra principalmente en la orientación de las disciplinas de soporte y la provisión de servicios de TI, que contribuyen a:

- Resolver de forma rápida los incidentes ocurridos en el servicio
- Conocer con precisión la configuración de los servicios y sus componentes.
- Realizar cambios de una forma segura y eficiente.
- Entender con claridad las necesidades del cliente, establecer acuerdos precisos y organizarse para ser capaces de cumplirlos.
- Mejorar el tiempo de provisión de servicios nuevos.
- Garantizar la robustez de los servicios críticos para el negocio.
- Controlar el desempeño de los suministradores contratados.

Contexto de la organización

La organización debe determinar los asuntos internos y externos que afectan a su capacidad para lograr los resultados previstos de su Sistema de Gestión de Servicios (SGS). Debe determinar las partes interesadas que son pertinentes al sistema de gestión de servicios, los límites y la aplicabilidad del SGS para establecer su alcance.

Liderazgo

La alta dirección debe asegurar que se establezcan la política y el logro de los objetivos de gestión de servicios, así como la disponibilidad de los recursos necesarios para contribuir a la eficacia y mejor continua del SGS y los servicios.

Política

La política de gestión de servicios debe comunicarse dentro de la organización y estar disponible a todas las partes interesadas. Esta política debe incluir:

- Los objetivos de gestión de servicios
- Compromiso para cumplir con los requisitos
- Mejora continua de los servicios.

Planificación

La organización debe determinar el impacto de los riesgos en la organización y las oportunidades para los servicios. Se deben planificar las acciones para tratar y mitigar los riesgos.

Objetivos de gestión de servicios y planificación

La organización debe implementar un plan de gestión de servicios. Se deben establecer objetivos de gestión de servicios que sean medibles y sean objeto de monitorización.

Apoyo

Es importante determinar y proporcionar los recursos humanos, técnicos, de información y financieros necesarios para el establecimiento del SGS. Por ello se debe asegurar la competencia de las personas y su implicación para el cumplimiento de los requisitos del SGS.

La organización debe determinar las comunicaciones internas y externas relevantes al SGS y los servicios.

La información documenta del SGG debe incluir:

- Alcance del SGS
- Política y objetivos de gestión de servicios
- Política de seguridad de la información y el plan de continuidad de los servicios.
- Catálogo de servicios.
- Acuerdos de nivel de servicio (SLA)

- Contrato con proveedores
- Gestión de riesgos

Operación

La organización debe mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe priorizar las peticiones de cambio y las propuestas de servicios nuevos o modificados para alinearse con las necesidades de negocio y los objetivos de gestión de servicios.

Gestión del catálogo de servicios. El catálogo de servicios debe incluir información para la organización, los clientes, los usuarios y otras partes interesadas para describir los servicios.

Gestión de activos. Asegurar que los activos para prestar el servicio están gestionados.

Gestión de la configuración. Definir los tipos de elementos de configuración (CI). Los servicios se deben clasificar como elementos de configuración (CI).

Gestión de relaciones con el negocio. Identificar y documentar los clientes, usuarios y otras partes interesadas de los servicios. La organización debe tener una o más personas designadas como responsables de la gestión de las relaciones con los clientes y del mantenimiento de su satisfacción.

Gestión de niveles de servicio. Para cada servicio prestado, la organización debe establecer uno o más SLA basados en los requisitos de servicio documentados. Los SLA deben incluir los objetivos de nivel de servicio, los límites de volumen de trabajo y las excepciones.

Gestión de proveedores. La organización debe acordar un contrato documentado para cada proveedor externo. Se debe evaluar la alineación de los objetivos de nivel de servicio u otras obligaciones contractuales con el proveedor externo frente a los SLA con los clientes, y tratar los riesgos identificados.

Presupuestos y contabilidad de servicios. Presupuestar y contabilizar servicios o grupos de servicios de acuerdo con sus políticas y procesos de gestión financiera.

Gestión de la demanda. Comprender la demanda de servicios actual y futura del cliente.

Gestión de la capacidad. Determinar, documentar y mantener los requisitos de capacidad para los recursos humanos, técnicos, de información y financieros teniendo en cuenta los requisitos de servicio y rendimiento.

Gestión de cambios. Registrarse y clasificarse las peticiones de cambio, incluidas las propuestas para incorporar, retirar o transferir servicios.

Gestión de incidencias. Determinar los criterios para identificar una incidencia grave. Las incidencias graves deben ser clasificadas y gestionadas de acuerdo a un procedimiento documentado.

Gestión de petición de servicio. Los registros de las peticiones de servicio se deben actualizar con las acciones llevadas a cabo durante las mismas.

Gestión de problemas. Analizar datos y tendencias sobre incidencias para identificar problemas. La organización debe llevar a cabo un análisis de la causa raíz y determinar las posibles acciones para prevenir la ocurrencia o repetición de las incidencias.

Gestión de la disponibilidad de servicios. Determinar los requisitos y objetivos de disponibilidad de los servicios. Los requisitos acordados deben tener en cuenta los requisitos de negocio relevantes, los SLA y los riesgos.

Gestión de la continuidad de los servicios. La organización debe crear, implementar y mantener uno o más planes de continuidad de los servicios.

Gestión de la seguridad de la información. La organización debe comunicar la importancia de cumplir con la política de seguridad de la información y su aplicabilidad al SGS y los servicios

Evaluación de desempeño

La organización debe evaluar el desempeño del SGS frente a los objetivos de gestión de servicios y evaluar la eficacia del SGS. implementar y mantener un programa o programas de auditoría. revisión por la dirección deben incluir decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambio en el SGS y los servicios. Se deben generar informes sobre el rendimiento y la eficacia del SGS y los servicios utilizando la información de las actividades del SGS y de la prestación de los servicios

Mejora

La organización debe determinar los criterios de evaluación a aplicar a las oportunidades de mejora cuando decida sobre su aprobación.

Cuando ocurra una no conformidad se debe:

- Hacer la revisión de la no conformidad
- Determinar causa raíz

Anexo III. Resumen de la Norma ISO/IEC 27013

ISO/IEC 27013

La relación entre la seguridad de la información y la gestión de servicios es tan estrecha que muchas organizaciones reconocen los beneficios de adoptar las Normas ISO/IEC 27001 e ISO/IEC 20000. Existen una serie de ventajas en la implementación de un sistema de gestión integrado que toma en cuenta no solo los servicios prestados sino también la protección de la información. Estos beneficios se pueden experimentar tanto si se implementa un estándar antes que el otro como si se implementan ambos estándares al mismo tiempo e incluyen:

- La confianza del cliente, en que se le proporcione un servicio eficaz y seguro.
- Menor costo de un programa integrado de dos proyectos con los que se consigue calidad del servicio y seguridad de la información.
- Reducción de implementación debido al desarrollo integrado de procesos comunes a ambos estándares.
- Mejora de la eficiencia operativa mediante la eliminación de duplicidad innecesarias.
- Mayor entendimiento entre los puntos de vista del personal de servicio y del personal de seguridad.
- Adoptar las mejores prácticas de ambas normas.

Una organización que está planificando implantar ambas normas puede encontrarse en una de estas tres situaciones:

- Todavía no ha implantado un sistema de gestión basado en alguna de ellas.
- Ya ha implantado un sistema de gestión basado en una de las dos.
- Ya ha implantado dos sistemas de gestión separados, cada uno de ellos basado en una de las normas, pero no están integrados.

La gestión de la seguridad de la información y la gestión de servicios abordan claramente procesos y actividades muy similares, al implementar un sistema de gestión integrado se debe considerar:

- Otros estándares o normas establecidos, por ejemplo, ISO 9001.
- Los servicios, procesos y sus interdependencias.
- Elementos de cada norma que puedan fusionarse

- Elementos que deben permanecer separados.
- El impacto o riesgos para los ser vivíos y la seguridad de la información
- Capacitación en el sistema integrado

Similitudes y diferencias entre ISO/IEC 27001 e ISO/IEC 20000

Una política aceptada comúnmente en la práctica impone el trato por separado de la gestión de los servicios y la gestión de la seguridad de la información. La razón más habitual aducida para tal separación es que los requisitos operacionales pueden tener prioridad sobre los problemas de seguridad.

Cuando se compara la gestión de la seguridad de la información y la gestión de los servicios de TI es fácil ver que cubren procesos muy similares, aunque un sistema de gestión remarque unos detalles más que otros.

Consideraciones sobre el alcance

Un área en la que los dos estándares difieren significativamente es en el ámbito de aplicación, cuáles son los activos, procesos y roles que deben ser destinados por el sistema de gestión.

Los alcances de los dos estándares se describen de manera diferente. La decisión sobre el orden en que se implementarán los dos sistemas de gestión debe basarse en las necesidades y prioridades del negocio. Tanto ISO/IEC 27001 como ISO/IEC 20000 pueden implementarse simultáneamente, si las actividades y esfuerzos de implementación pueden coordinarse y minimizarse la duplicación. El objetivo de la organización debería ser producir un sistema de gestión integrado viable que permita la conformidad con los requisitos especificados en ambas normas.

Ninguna organización debería tratar de crear un alcance combinado. Esto puede llevar a la mala aplicación de conceptos y a un desafío en el momento de validación.

En lo que se refiere a la documentación, se debería mantener la trazabilidad del sistema de gestión integrado con cada una de las normas por serado. Para reducir el esfuerzo, se puede crear un único conjunto de documentos para el sistema integrado.

Escenarios de implementación

a) No hay implantados otros sistemas de gestión

Se puede creer que cuando no hay implantados previamente estándares, cuando no hay políticas, procesos y procedimientos, la situación es más fácil de tartar, Desafortunadamente, esto es un

error. Es muy probable que las organizaciones que no tienen un sistema de gestión basado en ISO/IEC 27001 e ISO/IEC 20000 tengan algún otro sistema que deberá ser adaptado para conseguir la conformidad.
La decisión sobre qué sistema de gestión implementar y el orden en que deberían implementar, se debe basarse en las necesidades del negocio. La decisión podría incluir la conveniencia de tartar de implementar desde el principio un sistema de gestión basado en ambas normas o si, por el contrario, se comienza implantando una de ellas y después se procede con la otra. Aunque la implantación simultanea de los dos estándares se muestra como la mejor opción en la medida en que las actividades y esfuerzos de implementación pueden ser coordinados y la duplicidad minimizada, dependiendo de la naturaleza de la organización podría ser más prudente la implementación secuencial.

b) Existe un sistema de gestión que satisface los requisitos de una de las normas.

Donde ya se haya implantado un sistema de gestión que satisfaga los requisitos de una de las dos normas, el primer objetivo debería ser integrar los requisitos del otro estándar sin que sufra ninguna perdida de servicio y sin poner en peligro la seguridad de la información.

c) Existe dos sistemas de gestión, y cada uno satisface los requisitos de una de las normas

Es perfectamente posible que una organización tenga implantada la norma ISO/IEC 27001 en un área de la organización y la norma ISO/IEC 20000 en otra. En este caso se debería realizar una revisión para conseguir lo siguiente:

- Identificar y documentar los alcances existentes y los propuestos para el cumplimiento
- Comparar los dos sistemas de gestión existentes comprobando si existen aspectos mutuamente incompatibles.
- Empezar a involucrar a los interesados en ambos sistemas de gestión
- Planificar la mejor aproximación al sistema de gestión integrado.

Consideraciones para la implementación integrada

El objetivo de la organización debería ser la creación de un sistema de gestión integrado viable que permita cumplir con ambas normas, y no comparar ambas para determinar cuál es mejor o más correcta. El mejor sistema de gestión integrado es aquel que recoge lo mejor de cada norma y lo aplica adecuadamente, sin perder nada de lo que se necesario para cumplir con ambas

Al planificar la implementación integrada de ambos estándares, las organizaciones deben tener en cuenta cualquier diferencia en los criterios de riesgo y el impacto que estas diferencias tendrán en el tratamiento del riesgo. La organización debería adoptar uno de los enfoques que se describen a continuación:

- Utilice un enfoque común para la gestión de riesgos, incluida la evaluación de riesgos, para ambos estándares. Este es el enfoque más eficaz, ya que evita la duplicación de esfuerzos.

- Utilice metodologías de evaluación de riesgos independientes para los dos estándares. Si se elige esta opción, la organización debe usar una terminología que diferencie la evaluación de riesgos de la gestión de los servicios y la seguridad de la información.

- Utilizar un enfoque común para evaluar y tratar aquellos riesgos que afectan tanto la seguridad de la información como la gestión del servicio, y separar las metodologías de evaluación y tratamiento de riesgos para los riesgos que son específicos de la seguridad de la información y la gestión del servicio.

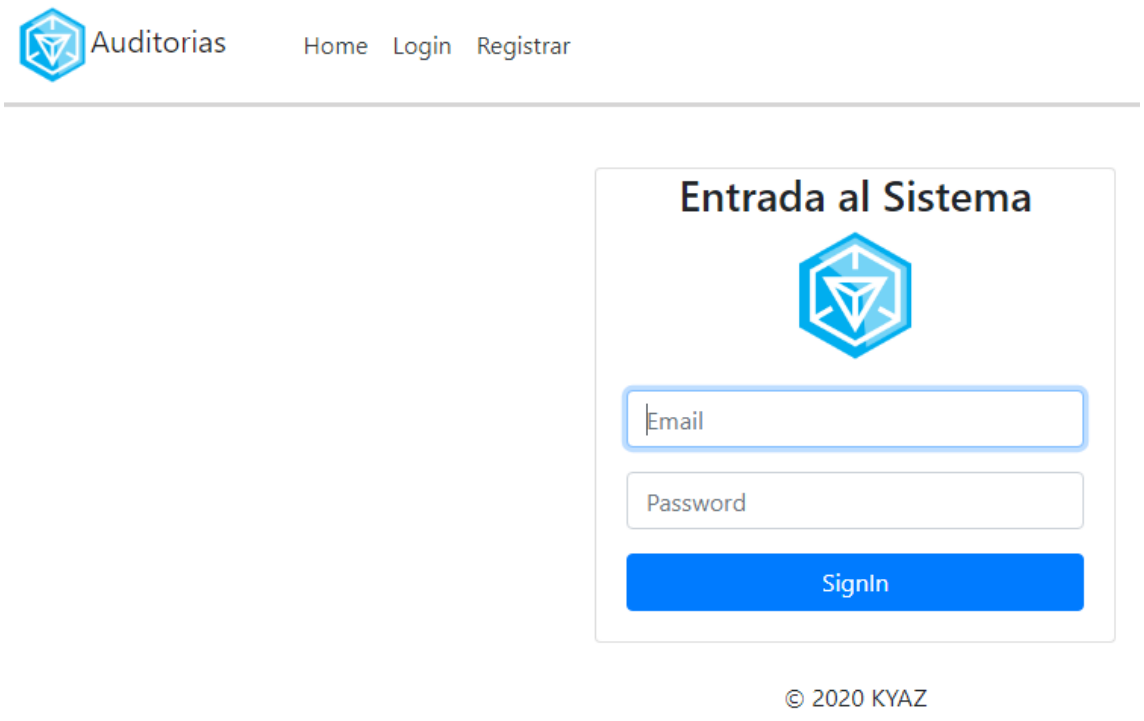
Anexo IV. Manual de usuario

El presente manual de usuario está organizado de acuerdo a la secuencia de pantallas del sistema de la siguiente manera:

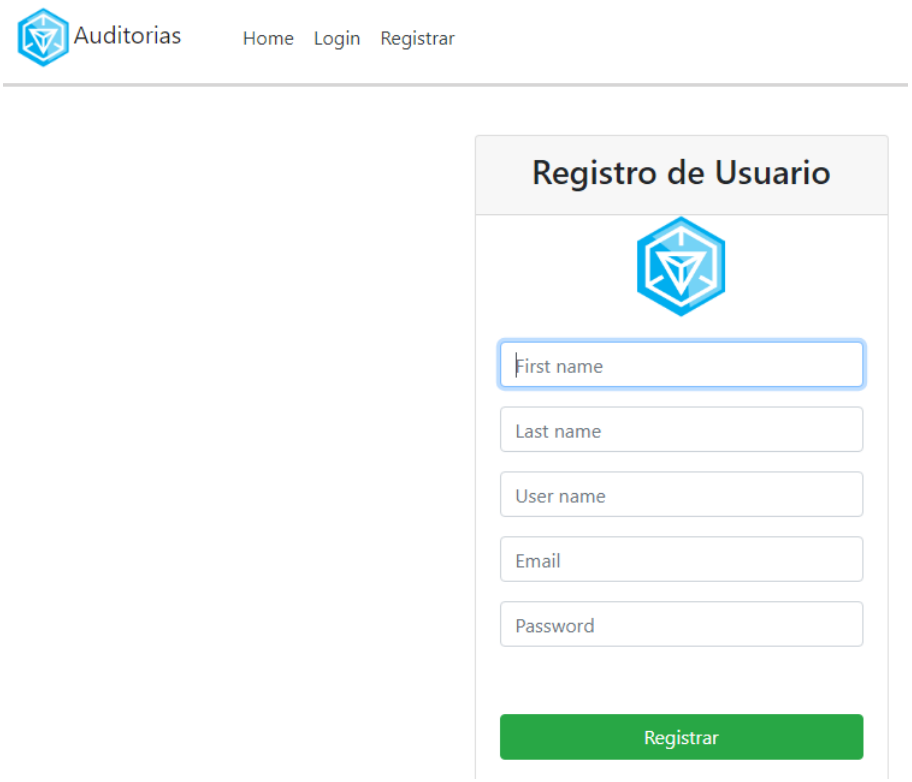
- Ingreso al sistema
- Registro cliente
- Realizar auditoría

1. Ingreso al sistema

En esta pantalla el usuario debe digitar su cuenta correo y contraseña, presionar sobre el botón SignIn, tal como se muestra en la siguiente figura. Los datos son los que se proporcionan al momento de registrarse.

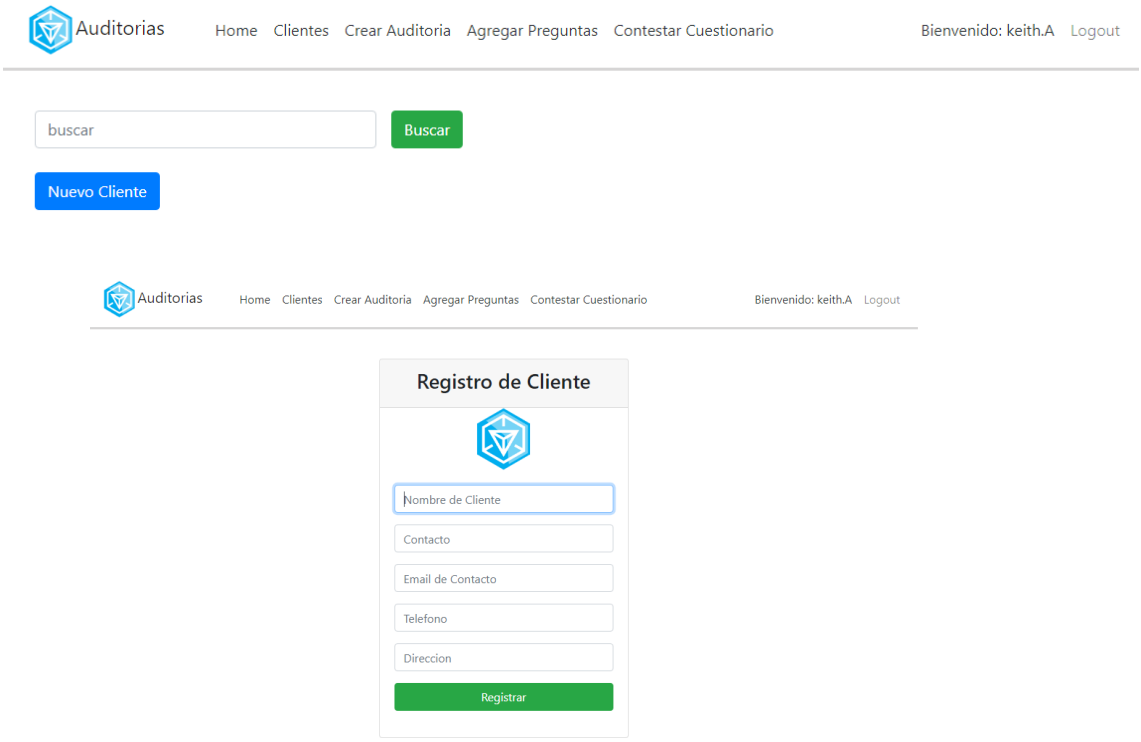


Si no está registrado, debe seleccionar Registrar en el menú principal, rellenar los datos para poder acceder al sistema y presionar sobre el botón Registrar



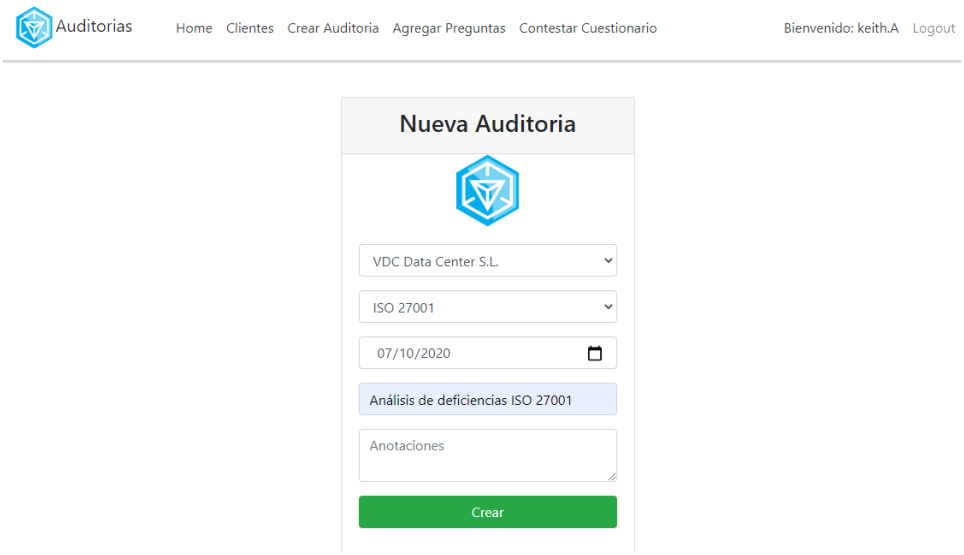
2. Registro de un cliente

Dar clic en Clientes, presionar el botón Nuevo Cliente, en la nueva ventana rellenar los campos para registrar los datos y presionar el botón Registrar.

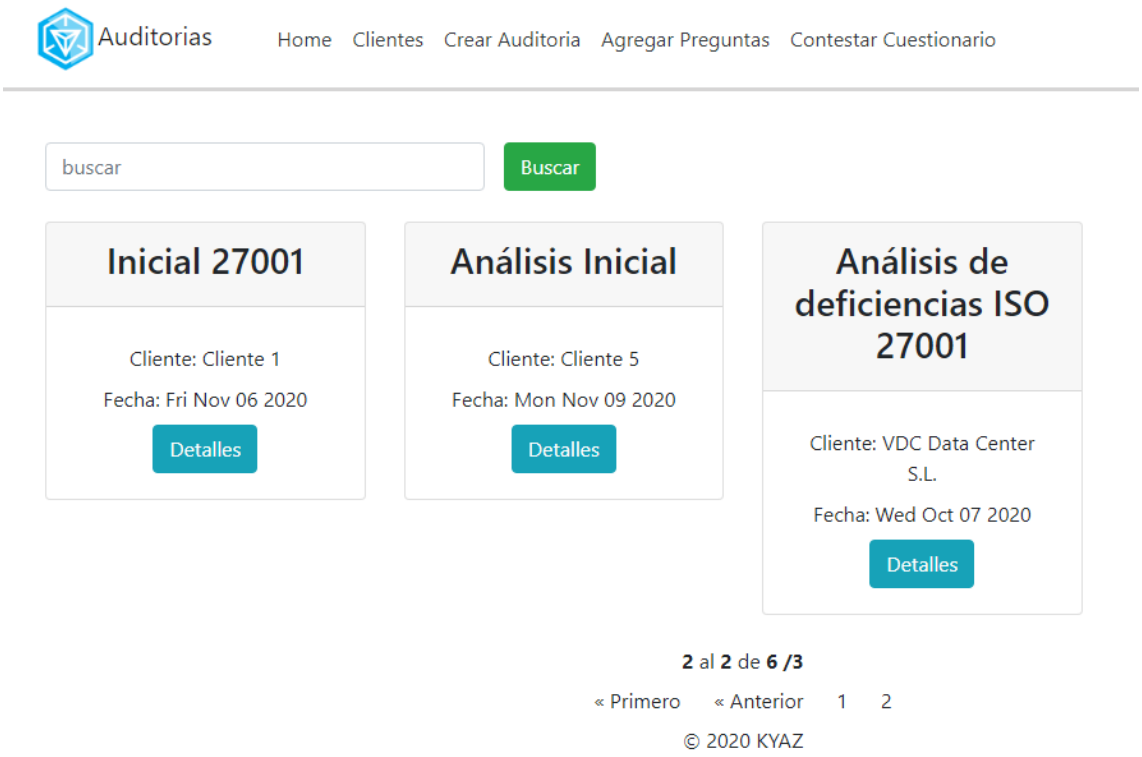


3. Crear auditoría

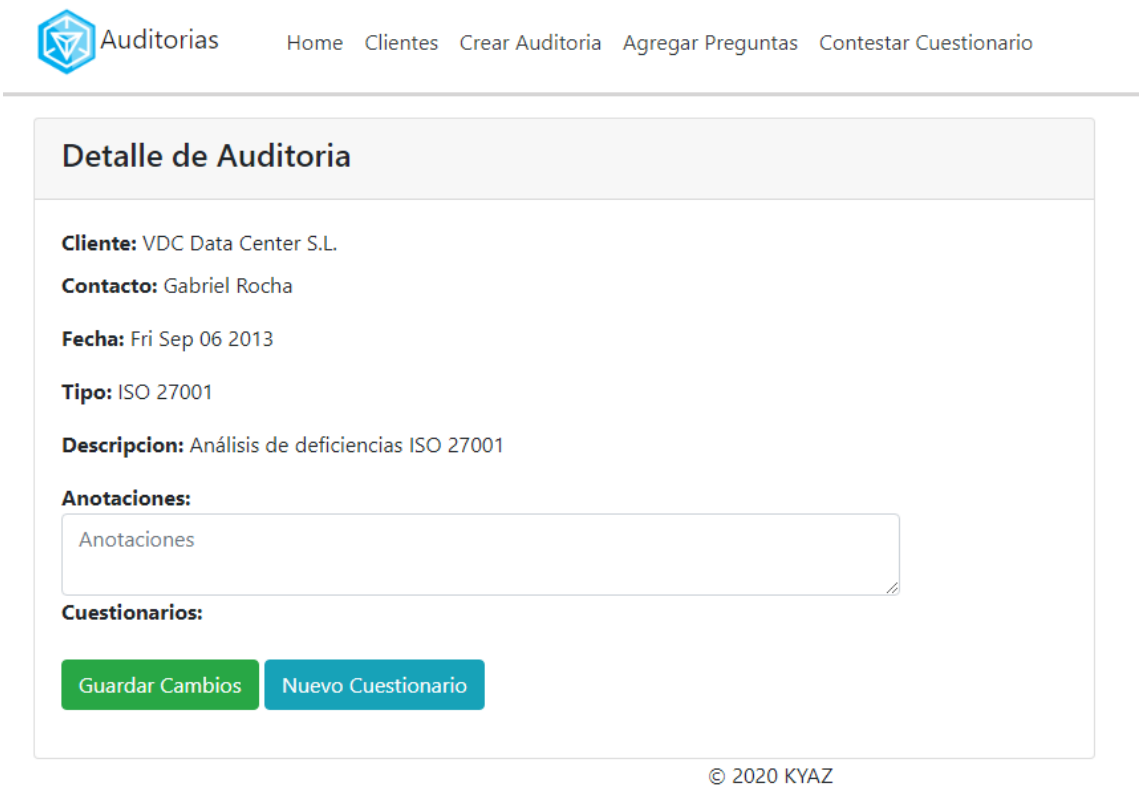
Para realizar el cuestionario, seleccionamos Crear Auditoría. El usuario debe rellenar los campos seleccionando el cliente del listado, tipo de auditoría (ISO27001 e ISO20000), fecha de la auditoría, descripción. Al presionar el botón Crear la aplicación volverá al menú principal.



En el menú principal mostrará la nueva auditoría que hemos creado, seleccionamos el botón Detalles.



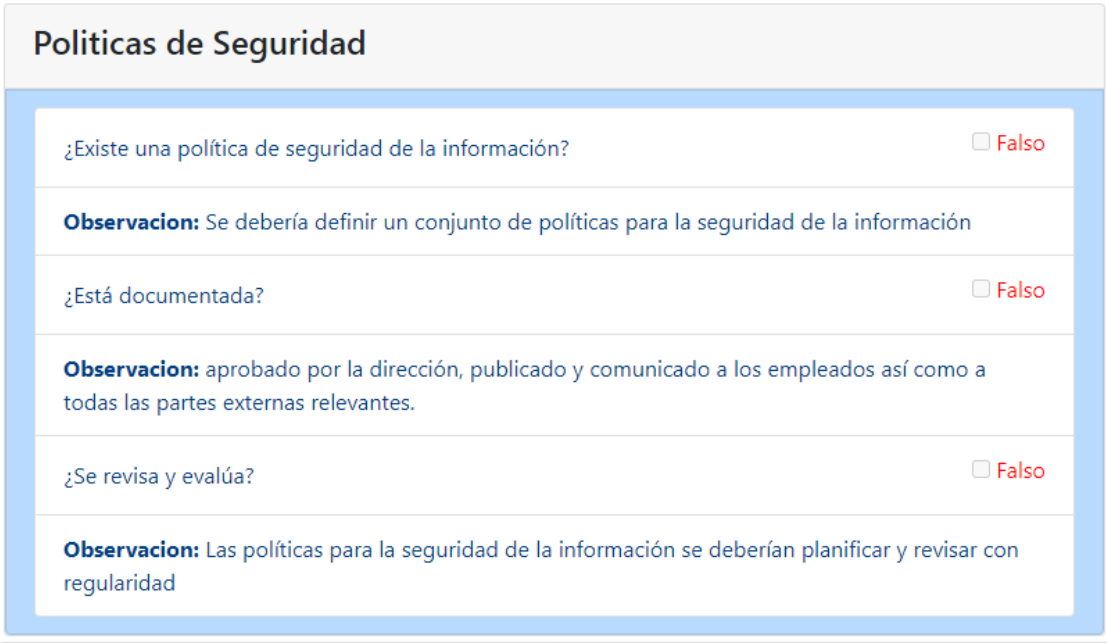
Al presionar sobre el botón detalles, se despliega una ventana en la que muestra el registro de la auditoría, presionamos el botón Nuevo Cuestionario.



Al presionar sobre el botón Nuevo cuestionario se despliega la ventana del formulario, esta ventana permite realizar el diagnostico de análisis de deficiencias. Debemos ponerle un nombre y fecha al cuestionario.

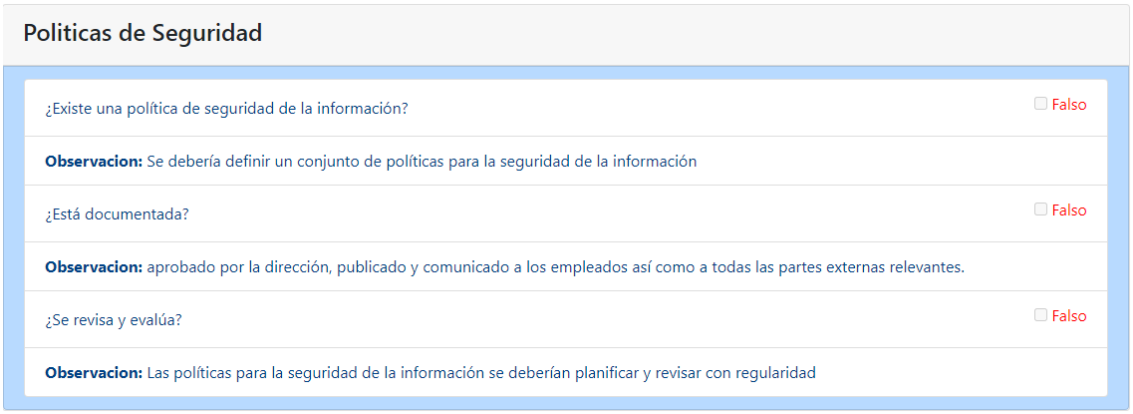
Para contestar el cuestionario debemos seleccionar verdadero o falso en cada pregunta, una vez finalizado presionamos el botón Guardar, y aparecerá el botón de Resultados.

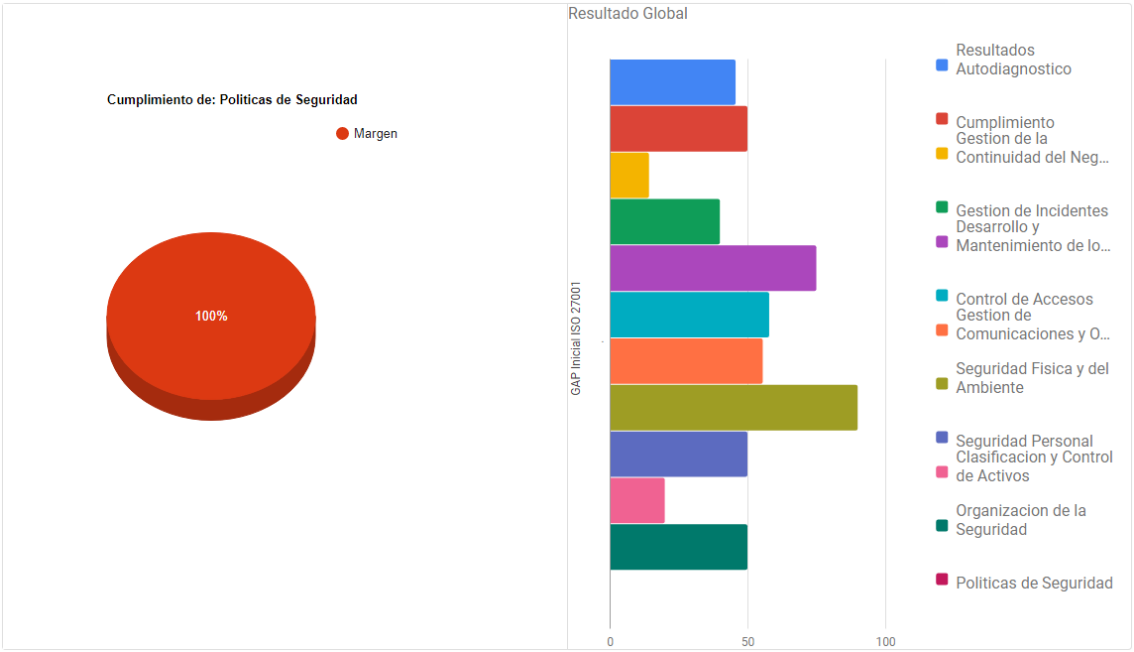
Al presionar sobre el botón Resultados, se despliega una ventana con el resultado de las preguntas contestadas. Mostrado la respuesta de cada dominio de la norma, con una observación, un diagrama de cumplimiento y el resultado global.



Anexo V. Resultados del diagnóstico de análisis de deficiencias

Se presentan un ejemplo de los resultados del diagnóstico del análisis de deficiencias realizado en el caso práctico, con algunos de los dominios evaluados según la norma ISO/IEC 27001.



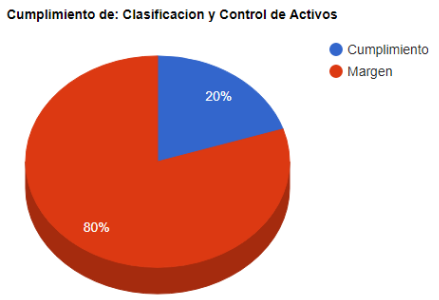


Organizacion de la Seguridad

¿La organización entiende qué es seguridad de la información?	Verdadero
Observacion: CUMPLE	
¿Existe un encargado de la seguridad de la información?	Falso
Observacion: Todas las responsabilidades de la seguridad de la información deben estar definidas	
¿Está la Gerencia involucrada con la seguridad de la información?	Falso
Observacion: Dirección debe alinear la seguridad de la información con los objetivos de negocio, para garantizar que la información de la organización está protegida adecuadamente	
¿Hay procedimientos escritos?	Falso
Observacion: Se debe estarbalecer un marco de gestión para controlar la seguridad de la información dentro de la organización	
¿Se revisa internamente los procedimientos?	Falso
Observacion: Los procedimientos de operación se deben documentar y revisar	
¿Existe una cooperación con terceros para las revisiones?	Falso
Observacion: La gerencia debe requerir a terceras personas que apliquen la seguridad en concordancia con procedimientos establecidos por la organización	
¿Se regula el acceso de terceros a la información?	Verdadero
Observacion: CUMPLE	
¿Existe alguna cláusula en los contratos con terceros sobre los riesgos/obligaciones/derechos/sanciones?	Verdadero
Observacion: CUMPLE	
¿Está regulada por vía contractual la subcontratación de la gestión de la información?	Verdadero
Observacion: CUMPLE	
¿Existe un encargado del mantenimiento de los equipos?	Verdadero
Observacion: CUMPLE	

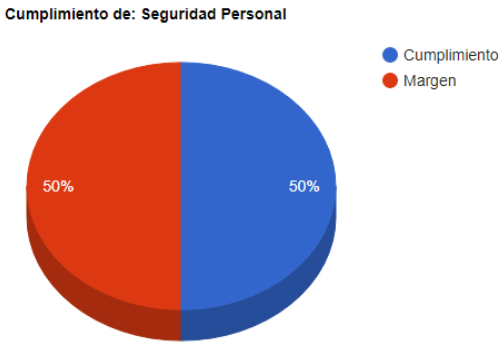
Clasificacion y Control de Activos

¿Existe una clasificación la información?	Falso
Observacion: Se debe asegurar que la información reciba un nivel de protección apropiado	
¿La información se maneja y almacena en función de su clasificación?	Falso
Observacion: Se debe aplicar procedimientos para el manejo de la información aprobado por la organización	
¿Existe un responsable de los accesos/disponibilidades/almacenamiento?	Verdadero
Observacion: CUMPLE	
¿Se ha realizado un inventario de los activos de información?	Falso
Observacion: Se deben identificar todos los activos y elaborar un inventario	
¿Está documentado y actualizado el inventario de activos?	Falso
Observacion: Se deben mantener y actualizar el inventario de todos los activos importantes	



Seguridad Personal

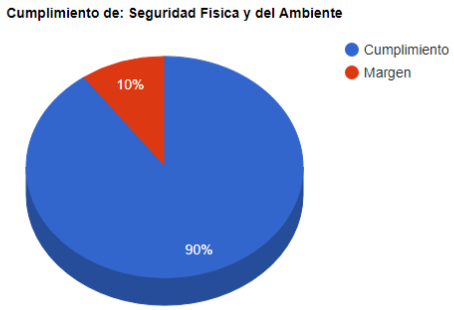
¿Está la seguridad incluida dentro de las responsabilidades de cada puesto de trabajo?	Falso
Observacion: Todas las responsabilidades de la seguridad de la información deben estar claramente definidas	
¿Se informa explícitamente a los empleados?	Falso
Observacion: Los roles y responsabilidades en seguridad de la información deben ser difundidos entre las partes implicadas	
¿Dentro de los contratos, existen acuerdos de confidencialidad?	Verdadero
Observacion: CUMPLE	
¿Existe formación a los empleados en materia de seguridad de la información?	Falso
Observacion: Todos los empleados de la organización deben recibir una adecuada capacitación en seguridad de la información	
¿Se emprenden acciones discplinarias?	Verdadero
Observacion: CUMPLE	
¿Se asegura la devolución de activos y retirada de permisos de acceso al finalizar la relación laboral?	Verdadero
Observacion: CUMPLE	



Seguridad Fisica y del Ambiente

¿Existe algun tipo de seguridad física?	☑ Verdadero
Observacion: CUMPLE	
¿Se protegen las instalaciones?	☑ Verdadero
Observacion: CUMPLE	
¿Es posible acceder a zonas críticas (CPD, archivo, etc.)	☑ Verdadero
Observacion: CUMPLE	
¿Se protege el equipamiento?	☑ Verdadero
Observacion: CUMPLE	
¿Están previstos fallos de suministros de energía?	☑ Verdadero
Observacion: CUMPLE	
¿Salen de la empresa equipos críticos?	☑ Verdadero
Observacion: CUMPLE	
¿Se controlan los equipos que estan fuera de la empresa?	☐ Falso
Observacion: Se debe controlar los equipos de trabajo fuera del local de la organización	

¿Se elimina/recicla/almacena el equipamiento obsoleto?	Verdadero
Observacion: CUMPLE	
¿Existe algún control sobre la información disponible en archivos/escritorios/estanterías/ordenadores/copias impresas?	Verdadero
Observacion: CUMPLE	
¿Se elimina información (documentos impresos, etc) de forma segura?.	Verdadero
Observacion: CUMPLE	



Gestion de Incidentes

¿Existe un procedimiento de incidencias? Es formal, por escrito?	Falso
Observacion: Se debe asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información	
¿Se comunican las incidencias?	Verdadero
Observacion: CUMPLE	
¿Se gestionan las incidencias?	Verdadero
Observacion: CUMPLE	
¿Existe documentación histórica de las incidencias?	Falso
Observacion: Es necesario detectar problemas subyancentes indicados por repetición de incidentes de seguridad	
¿Se actúa para evitar repeticiones de las incidencias?	Falso
Observacion: Se debe establecer mecanismos para permitir cuantificar los tipos de los incidentes en la seguridad de la información