UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

PROGRAMA DE TITULACIÓN POR TESIS

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO INFORMÁTICO

PRESENTADO POR:

Bach. GRANADOS NECIOSUP, PAOLA DEL ROSARIO

Bach. PEREZ PARRA, KEYLA MARTHA

ASESOR: MSc. LINÁREZ COLOMA, HUMBERTO VICTOR

LIMA - PERÚ

2019

DEDICATORIA

Dedico esta tesis principalmente a Dios, por iluminar mí camino.
A mis padres, por la ayuda que siempre me brindan, a mis hermanos y a mis amigos que siempre me apoyan y están a mi lado

Paola del Rosario Granados Neciosup

Esta tesis la dedico a mi madre, es la persona más importante en mi vida y la que siempre me apoya, a mi padre que, aunque este lejos, siempre me apoyó en terminar la carrera.
A mis hermanos, porque he aprendido mucho de ellos y siempre están allí cuándo más los necesito y a las personas de que una u otra manera siempre estuvieron allí.

Keyla Martha Perez Parra

AGRADECIMIENTO

Agradecemos a nuestras familias por brindarnos apoyo incondicional, a nuestros profesores, que nos transmitieron sus conocimientos y enseñaron a seguir creciendo en nuestra carrera.

Un agradecimiento especial a nuestro asesor, a lo largo de nuestra carrera universitaria nos enseñó varias materias, y nos guio y apoyó en el desarrollo de nuestra tesis.

Paola Granados y Keyla Perez

ÍNDICE GENERAL

INDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este trabajo se realizó con el principal objetivo de obtener el título de ingeniero informático, teniendo como título de tesis “Facilitar el cumplimiento de la ISO 27001 mediante una herramienta de tecnología workflow” con la cual se ayudó y/o facilitó al cumplimiento de las buenas prácticas en seguridad de la información, bajo la norma ISO/IEC 27001:2013 y las etapas del modelo Deming (Plan-Do-Check-Act), además ayudó al cumplimiento de los controles para la protección de los activos de información, protegiéndola de un amplio rango de amenazas, teniendo en cuenta que la información adopta diversas formas, ya que puede estar impresa o escrita, en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en una conversación.

Como objeto de estudio para la elaboración del sistema se tomó como referencia a la empresa “Industrias Triveca SAC”, la cual se encarga de brindar soluciones de agua potable en el sector de alcantarillado. En dicha empresa se realizó una rápida visita a sus áreas administrativas y algunas entrevistas, y se obtuvo como resultado la falta de capacitaciones en seguridad de la información y políticas para salvaguardarla, además presentaron problemas de pérdida de información. Por ello la gerencia indicó la necesidad de contar con una herramienta para facilitar el cumplimiento de las buenas prácticas de seguridad de la información a fin de poder mantener la confidencialidad, disponibilidad e integridad de los activos de información. Además, enfatizó la necesidad de que el personal sea capacitado en temas referidos a seguridad de la información.

Palabras clave: ISO 27001, activo de información, buenas prácticas, Tecnología workflow, modelo Deming, disponibilidad, integridad, confidencialidad.

ABSTRACT

This work was carried out with the main objective of obtaining the degree of computer engineer, having the thesis title “Facilitate compliance with ISO 27001 through a workflow technology tool” with which it helped and / or facilitated the fulfillment of good Information security practices, under ISO / IEC 27001: 2013 and the stages of the Deming model (Plan-Do-Check-Act), also helped to comply with the controls for the protection of information assets, protecting it from a wide range of threats, taking into account that the information takes various forms, since it can be printed or written, on paper, stored electronically, transmitted by mail or by electronic means, shown on video or spoken in a conversation.

As a study object for the elaboration of the system, the company “Industrias Triveca SAC” was taken as a reference, which is responsible for providing potable water solutions in the sewerage sector. In this company, a quick visit to its administrative areas and some interviews was carried out, and as a result, the lack of training in information security and policies to safeguard it, they presented problems of loss of information. Therefore, management indicated the need for a tool to facilitate compliance with good information security practices in order to maintain the confidentiality, availability and integrity of information assets. In addition, he emphasized the need for staff to be trained on issues related to information security.

Keywords: ISO 27001, information asset, good practices, Workflow technology, Deming model, availability, integrity, confidentiality.

INTRODUCCIÓN

En los últimos años con el desarrollo de la tecnología, la información se ha convertido en uno de los activos más importantes dentro de una organización, pudiendo estar presente en múltiples formatos: escrita o impresa en papel, almacenada electrónicamente por medio de correos, ilustradas en películas, transmitida por alguna tecnología de comunicación, entre otros. Los riesgos de seguridad se han intensificado procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La información de cualquier organización constituye uno de los activos más importantes para la compañía, por lo tanto, debe ser utilizada dentro de un adecuado entorno de seguridad, cualquiera que sea el medio en el que se encuentre (físico o lógico) y el ambiente tecnológico en que se procese.

Se es consciente de que la seguridad de la información es principalmente un proceso administrativo, relacionado y dependiente de aspectos tecnológicos. Por esta razón, se establece un compromiso mediante el desarrollo de un modelo de soporte para la gestión y la promoción de una cultura de seguridad, definiendo las responsabilidades por parte de su personal, clientes y usuarios, para la protección de la seguridad de sus activos de información.

Es una decisión gerencial y estratégica, implantar su Sistema de Gestión de Seguridad de la Información, el cual le permite brindar a sus funcionarios, clientes y socios de negocio, niveles apropiados de seguridad y protección de la información.

A continuación, se muestra la estructura del proyecto:

Capítulo 1: Visión del proyecto, en el cual describe los antecedentes del problema, el negocio y la identificación de la problemática.

Capítulo 2: Marco Teórico, donde se identifican las bases teóricas, metodologías a usar y los sistemas existentes en el mercado.

Capítulo 3: Desarrollo del proyecto, en el cual se muestra el alcance del proyecto donde se muestra el cronograma, las restricciones, exclusiones y supuestos del proyecto.

Capítulo 4: Desarrollo del producto, en el cual se muestra el modelado de negocio, los requerimientos, el análisis, diseño y la arquitectura del producto.

Conclusiones y recomendaciones, donde se sintetiza los resultados del proyecto, de acuerdo al alcance de los objetivos.

CAPÍTULO 1: VISIÓN DEL PROYECTO

1.1. Antecedentes del problema

Hace algún tiempo no se hablaba en certificar los procesos, hasta que el año 2000 la ISO 9000 generó tendencia en la certificación de los sistemas de gestión de calidad, mediante la norma ISO 9001:2000.

Sin embargo, no había una norma que certificara las buenas prácticas de seguridad de la información, sino que hasta el 2005 el estándar conocido era la ISO 17799 pero con la limitante de ser un "código de prácticas", con ello se le da un nuevo alcance a la seguridad informática, ya que no sólo eran buenas prácticas sino establece un estándar certificable y que brinda una ventaja competitiva en las organizaciones.

Para el presente trabajo se ha tomado como referencia la norma ISO/IEC 27001:2013 la cual nos da una guía específica de los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) ya que consideramos que es una guía más completa.

1.1.1. El negocio

Industrias Triveca S.A.C. nace en el año 1987, en el distrito de San Miguel, departamento de Lima, solo con capitales peruanos. Posteriormente traslada sus oficinas a los distritos de Santiago de Surco y en Lurín, en donde se encuentra la planta de producción de plásticos y el laboratorio de medidores de agua.

Actualmente cuenta con oficinas administrativas, de comercialización y de proyectos en los departamentos de Loreto, Lambayeque, Piura y Tumbes.

Industrias Triveca S.A.C., con 29 años de experiencia en el mercado nacional, ha logrado consolidarse como una empresa especializada en brindar soluciones al sector de agua potable y alcantarillado, así como a empresas del sector industrial, construcción, minero, petrolero, agroindustrial, alimentario y pesquero. Dichas soluciones comprenden desde el suministro de equipos, productos y su puesta en marcha, hasta la administración de servicios básicos como: Gestión Comercial, Gestión Operacional, Automatización y Telemetría.

Con respecto a la organización de Industrias Triveca S.A.C. (ver figura N°1), se realiza de la siguiente manera:

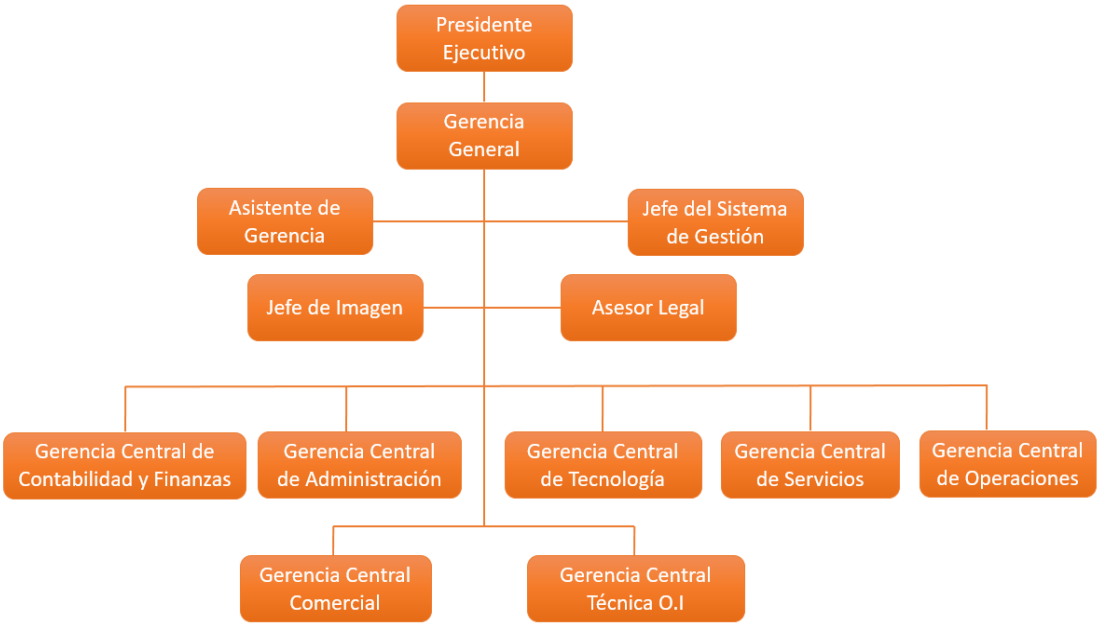


Figura N° 1 Organigrama de Industrias "Triveca S.A.C."

Fuente: Industrias Triveca SAC

Misión:

Satisfacer las necesidades de nuestros clientes ofreciendo soluciones integrales e innovadoras, respaldando en el talento, el compromiso y la experiencia de nuestros colaboradores.

Visión:

Ser líderes en el mercado nacional del sector saneamiento a través de nuestras soluciones.

Soluciones integrales

Ofrecen un portafolio completo de soluciones integrales a los sectores de agua potable y saneamiento, industrial, construcción, minero, entre otros, sobre la base de relaciones sólidas, experiencias reales, profesionales altamente calificados, instalaciones diseñadas e implementadas para el logro de excelentes resultados.

Líneas de producto

Cuentan con seis líneas de productos que constituyen el soporte de sus soluciones integrales para optimizar la gestión de los procesos comerciales y operacionales en las empresas prestadoras del servicio de agua potable y saneamiento (EPS), las que contribuyen a la reducción del agua no facturada (ANF): medición, verificación inicial de medidores de agua, accesorios marca Triveca, instrumentación y automatización, tratamiento y servicios de tercerización (comercial y redes).

Medición: Se orienta a la medición y control de fluidos en conexiones de agua potable, tanto domésticas como industriales. Destaca su micro medidores y macro medidores HOMOLOGADOS por la Dirección de Metrología del Instituto Nacional de la Calidad (INACAL), y según las normas nacionales e internacionales vigentes.

Accesorios: Ofrecen una variedad de productos marca Triveca para conexiones de agua, sistemas contra robo o manipulación de medidores, entre otros, fabricados en su planta industrial ubicada en Lurín. Asimismo, comercializamos sistemas de corte intrusivo como mecanismo de persuasión de pago de los usuarios morosos.

Verificación inicial de medidores de agua: Cuentan con un laboratorio para la verificación inicial de medidores de agua potable que forma parte del Organismo de inspección Tipo C, acreditado por la Dirección de Metrología del Instituto Nacional de la Calidad (INACAL) bajo la NTP-ISO 17020:2012.

Instrumentación y automatización: En instrumentación brindan soluciones integrales para la medición de flujo, nivel, presión y de otros parámetros que requieren ser medidos en el sector de aguas e industrial. Destacan los instrumentos de medición de caudal, presión, fugas en redes, gases y para la disminución de la pérdida de agua. En Automatización controlamos y monitoreamos los proyectos de automatización y telemetría con tecnología de última generación a un tiempo real y desde cualquier lugar del mundo a través de la tecnología de comunicación celular (GPRS), radiofrecuencia e Internet. Destacan los sistemas automatizados SCADA.

Tratamiento: Brindamos soluciones integrales para el tratamiento de agua y la eliminación de olores con tecnología de punta de la firma Italiana Sodi Scientifica y la firma americana Integrity Municipal Systems. Destacan los sistemas para la eliminación de olores en cámaras de desagüe. Además, ofrecemos soporte técnico de manera permanente.

Servicios de tercerización: Ofrecemos servicios de tercerización (comercial y redes) en apoyo a la gestión comercial y operacional con personal altamente calificado y en constante capacitación para lograr optimizar los procesos de las EPS y en busca de la mejora continua en beneficio de los usuarios del servicio de agua, de tal manera que este se vea reflejado en el incremento de la facturación de las EPS y en la erradicación del agua no facturada.

1.1.2. Procesos del negocio

Con respecto a los procesos que se desarrollan en Industrias "Triveca S.A.C." (Ver Figura N° 2) se tiene lo siguiente:

Figura N° 2 Mapa de procesos de Industrias Triveca SAC

Fuente: Área de TI, Industrias Triveca SAC

El proceso involucrado en el proyecto es:

Procesos de apoyo:

Los procesos de apoyo son los que apoyan o soportan los procesos operativos, sus clientes son internos. En Triveca estos procesos son: asuntos legales, gestión de contabilidad y finanzas, gestión de soporte informático y gestión de recursos humanos. Los procesos de soporte también reciben el nombre de procesos de apoyo.

El proceso en el cual nos enfocaremos es la gestión del soporte informático

<u>Gestión de soporte informático:</u>

Dentro del procedimiento de gestión informático, se encuentra la creación de usuarios y correos electrónicos, la baja de usuarios, la asignación de equipos, la asistencia y soporte, actualización de inventario de equipo, monitoreo de equipos, actualización de sistemas operativos, administración de servicio de correo electrónico.

Para este proceso se ha desarrollado el macroproceso (Ver figura N° 3) de Sistema de Gestión de Seguridad de la Información (SGSI) para la compañía:

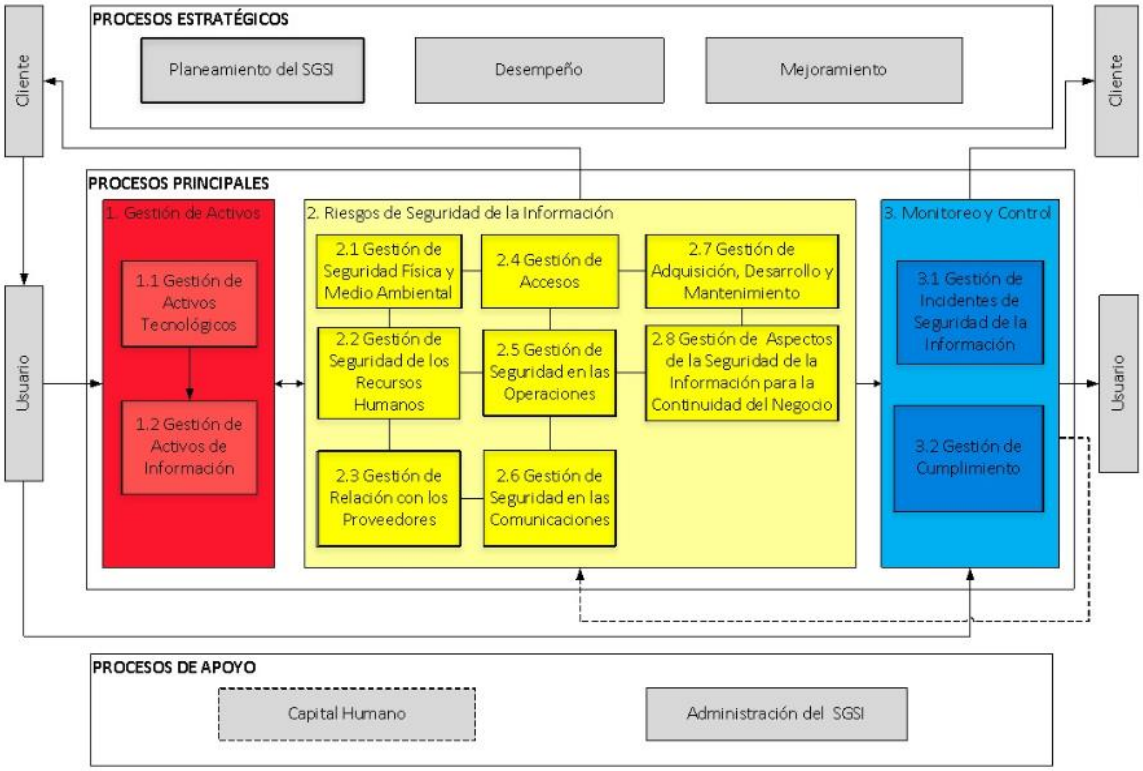


Figura N° 3 Mapa de procesos del SGSI
Fuente: Elaboración propia.

a) Procesos estratégicos

I. **Planeamiento del SGSI:** Este proceso está abocado principalmente a planificar el Sistema de Gestión de Seguridad de la Información (SGSI). Esta planificación implica la determinación y difusión de la Política de Gestión del SGSI de la organización y de los Objetivos del SGSI, así como la planificación de los procesos identificados en el mapa de procesos, que son necesarios para cumplir los objetivos del SGSI y los controles establecidos por la organización.

II. **Desempeño:** Involucra a quien revisa el resultado del desempeño del SGSI y sus procesos. Así mismo, el Representante de la Dirección, en coordinación con el Jefe de Gestión planifican y aseguran el desarrollo de auditorías internas que permiten medir el desempeño y eficacia del SGSI, a fin de tomar las acciones pertinentes.

III. **Mejoramiento:** Este proceso involucra a la alta dirección que planifica y ejecuta las revisiones periódicas del Sistema de Gestión de Seguridad de la Información. Así como también al Representante de la Dirección, quien en coordinación con el Jefe de Seguridad TI, aseguran la gestión y priorización de las acciones correctivas y otras mejoras a fin de lograr la mejora continua del SGSI.

b) Procesos Principales:

I. **Gestión de Activos:** Este proceso asegura que todos los activos de información sean identificados, inventariados, además de clasificarlos y definir las responsabilidades y controles para su protección de acuerdo a su importancia en la organización.

II. **Gestión de Riesgos de SI:** Este proceso de asegurar la planificación, implementación y control de los procesos necesarios llevando a cabo evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se den cambios. Así mismo, asegura la implementación de un plan de tratamiento de riesgos de seguridad de la información.

III. **Monitoreo:** Este proceso abarca evaluar el desempeño de la seguridad de la información respecto a los controles definidos para los riesgos de seguridad de la información.

c) Procesos de Apoyo:

I. **Capital humano:** Este proceso a quien es responsable de evaluar el desempeño del área de Gestión de Desarrollo Humano (proveedor del SGSI), lo cual está orientado a asegurar la competencia e idoneidad del personal que participa en los procesos del Sistema de Gestión, manteniendo dicha competencia a través de actividades relacionadas a la capacitación.

Así mismo, las jefaturas de área de la organización se aseguran internamente que el personal nuevo sea consciente de sus funciones, responsabilidades, de la importancia del SGSI, entre otros temas, para lo cual realizan la inducción del personal nuevo. Además se ha designado internamente a un Gestor de Capacitaciones quien en coordinación con las jefaturas de área y con el Vicepresidente de Soluciones de Negocio Tecnológicas gestiona la ejecución de capacitaciones específicas para asegurar adicionalmente la competencia de los colaboradores.

II. **Administración del SGSI:** Este proceso involucra al Representante de la Dirección y el Jefe de Gestión de Aseguramiento de Calidad, quienes se encargan de mantener el sistema de control documentario y de registros del Sistema de Gestión de Seguridad de la Información.

1.1.3. Descripción del problema

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las empresas de cualquier sector deben tomar decisiones rápidas y eficientes ya que se encuentran propensos a múltiples ataques hacia sus vulnerabilidades, esto convierte la información en uno de los activos más importantes dentro de las organizaciones. Visto este concepto, debemos que proteger la integridad, confidencialidad y disponibilidad de la información (ver Figura N° 4) en todas sus formas ya sea física, electrónica, etc.

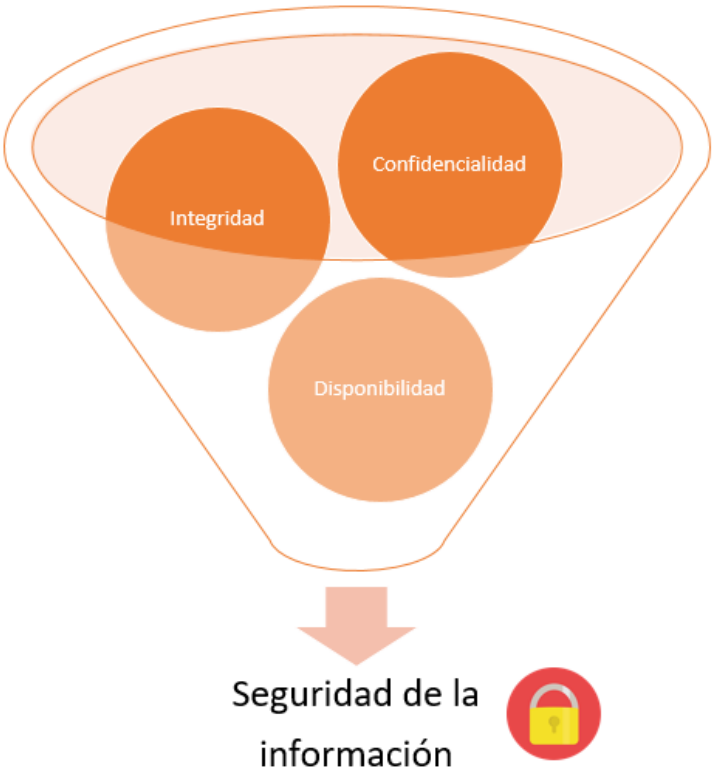
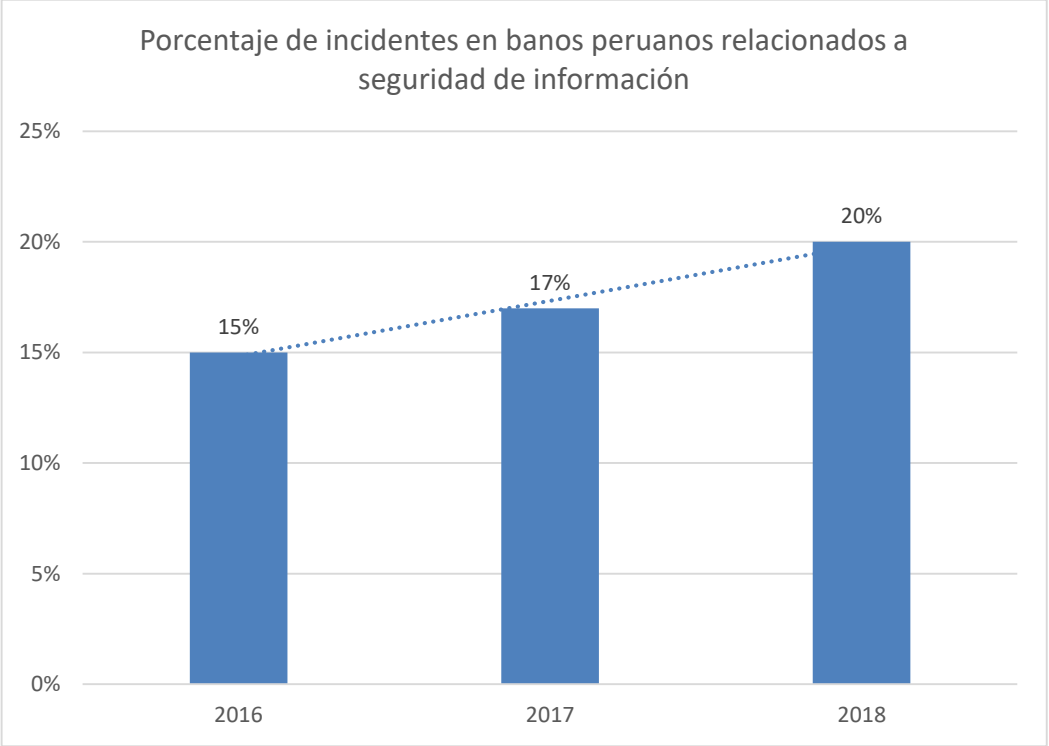


Figura N° 4 Principios de Seguridad de Información
Fuente: Elaboración propia.

Actualmente la empresa Industrias Triveca SAC cuenta con una ineficiente gestión de buenas prácticas de seguridad de la información lo que conlleva a un descontrol de sus activos de información, tales como documentos, software, dispositivos físicos, imagen, reputación y servicios que se encuentran expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes. Además, de ello y en conjunto con las múltiples vulnerabilidades que existen y que presentan en la organización para almacenar, mantener, transmitir y recopilar información, y que podrían afectar la confidencialidad, disponibilidad e integridad de la información vital para la organización, el negocio y los clientes.

Añadido a ello la falta de conocimiento y concientización del valor de la información y el nivel de importancia para la empresa lleva a que se encuentre vulnerada por las distintas amenazas. Sin mencionar la exposición y robo de la cual podría ser víctima la empresa.

Tabla 1: Incidentes relacionados a seguridad de información



Fuente: Elaboración propia.

Por otro lado se presenta la ausencia de las políticas de seguridad de la información, que aumenta la probabilidad de ocasionar daños a las organizaciones no sólo económicas, sino de reputación, cómo por ejemplo; se han presentado casos en el 2018 de bancos peruanos que sufrieron ataques a sus sistemas (Ver tabla 1) y de los que perdieron no sólo información importante para sus operaciones sino que según Gaetano Capurro (2019), especialista de riesgos de JLT Perú, reveló que "las pérdidas mundiales por ataques cibernéticos alcanzan anualmente los US$ 400,000 millones aproximadamente".

Es por ello que las empresas peruanas y por ende, industrias Triveca, presentan varias brechas de seguridad de la información, además de la falta de capacitaciones a su equipo para encontrar y resolver cualquier problema de esta índole y concientización de sus colaboradores, ya que no sólo es responsabilidad del área de seguridad de información o tecnología, sino toda la empresa.

El anexo A de la 27000 (ver figura N° 5) indica controles por cada uno de los ámbitos de una organización para salvaguardar la información, desde el ámbito de los recursos humanos hasta la seguridad del cumplimiento legal.

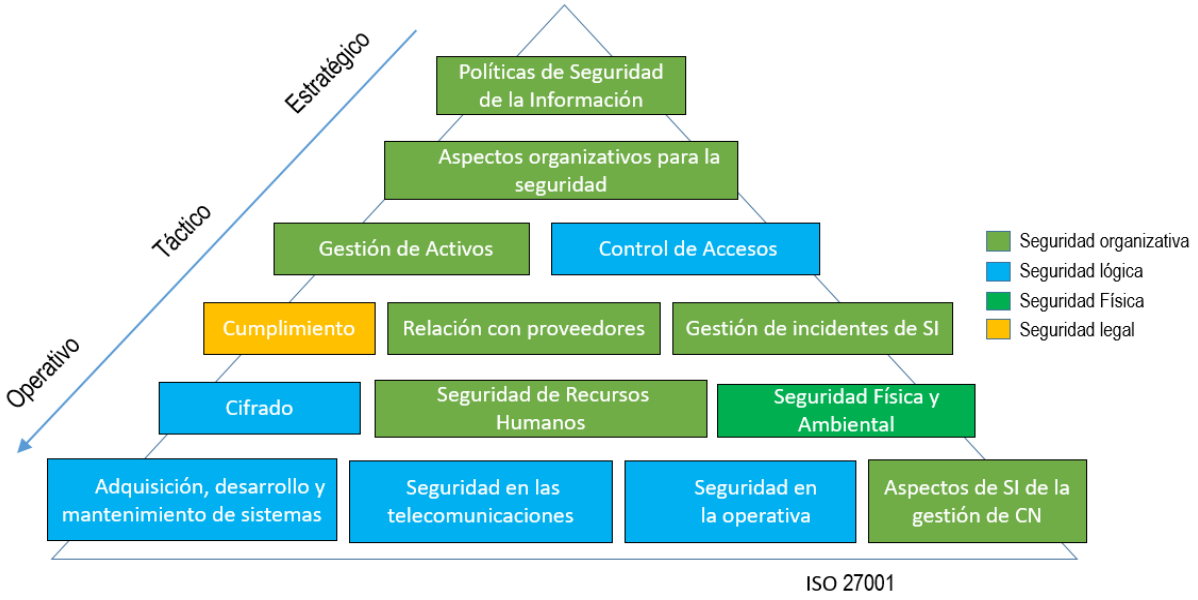


Figura N° 5: Dominios del anexo A, según 27000
Fuente: Elaboración propia

1.2. Identificación del problema

1.2.1. Problema principal

Para Industrias "Triveca S.A.C" el problema principal identificado es la ineficiente gestión en las buenas prácticas de seguridad de la información en la organización, ya que se ha identificado que muchos colaboradores e incluso personal del área de soporte no tiene conocimiento del tratamiento de incidentes de seguridad de la información.

1.2.2. Problemas específicos

a) Descontrol de los activos de información
b) Falta de políticas y procedimientos para el resguardo de la información.
c) Riesgos de pérdida de la información por falta de conocimiento de buenas prácticas en seguridad de la información.
d) Falta de concientización en temas de seguridad de la información por parte de los colaboradores de la empresa.
e) Desconocimiento de la protección de los activos de información de acuerdo con su nivel de importancia.

1.3. Objetivos

1.3.1. Objetivo general

El objetivo general de este proyecto de tesis es conseguir una eficiente gestión en las buenas prácticas de seguridad de la información en la organización.

1.3.2. Objetivos específicos

a) Controlar adecuadamente los activos de información.
b) Manejar y controlar políticas y procedimientos para el resguardo de los activos de información.
c) Conocer las buenas prácticas de la información según la ISO 27001.
d) Concientizar a los colaboradores acerca de seguridad de la información.
e) Clasificar los activos de información de acuerdo a su nivel de importancia.

1.4. Descripción y sustentación de la solución

En este punto se describe el planteamiento de la solución para el problema principal, para tener una gestión en las buenas prácticas de seguridad de la información en la organización.

1.4.1. Descripción de la solución

La solución planteada es un sistema workflow en Bizagi que realiza el checklist del cumplimiento según la norma, ello se plasma de la siguiente manera:

a) Elaboración de un módulo de mantenimiento**:**
   El módulo permite gestionar un perfil de auditor, analista TI, jefe de seguridad TI, dueño del sistema de gestión (gerente general).
b) Elaboración de un módulo para gestionar la normativa**:**
   El módulo permite la gestión de la normativa de la ISO 27001, que abarca desde el requisito “4 Contexto de la organización” hasta “10 Mejora Continua”.
c) Elaboración de un módulo para gestionar evidencias:

El módulo permite gestionar evidenciar que se realice lo indicado dentro del módulo de normativa. Revisión y aprobación de los informes (hallazgos encontrados).

d) Elaboración de un módulo de auditoría:

   El módulo permite la gestión de los informes de auditoría, según la revisión de los resultados obtenidos en la revisión del módulo de evidencias. Aprobación del informe de auditoría por parte del representante de la alta dirección (Acta de conformidad).

1.4.2. Justificación de la realización del proyecto

La importancia de realizar este proyecto es que el sistema facilita el cumplimiento de las buenas prácticas de la ISO 27001 ayudando así a disminuir las vulnerabilidades de seguridad; debido a los riesgos a los que están expuestos los activos de información.

Es por ello que la implementación de un SGSI, brinda los procedimientos para identificar y evaluar los riesgos, las vulnerabilidades de la información y sabiendo esto se va a implementar los controles necesarios para resguardar los activos de información.

Beneficios tangibles:

a) Reducir la pérdida de información al Monitorear y gestionar de manera eficiente las vulnerabilidades de la seguridad de la información, para reducirlos en un 90% de acuerdo a la pérdida de información.

Beneficios intangibles:

a) Mejorar el prestigio de la empresa.
b) Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
c) Concientizar a los colaboradores acerca de la seguridad de la información de la compañía y la información personal.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Marco conceptual

2.1.1. Sistemas de Gestión de Seguridad de la información

Gómez Fernández & Andrés Álvarez (2009) lo define:

> Un sistema de gestión de seguridad de la información es una parte del sistema de gestión general con un enfoque de riesgo empresarial, que tiene como finalidad crear, implementar, controlar, examinar, mantener y mejorar la seguridad de la información. Esto significa que se comenzará a tener control sobre lo que pasa en los sistemas de información y sobre la información que se maneja en la organización. A la vez nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore. (p. 77).

La norma ISO 27001 indica que el SGSI comprende tanto la organización como las políticas, procedimientos, la planificación, los procesos y recursos. Es decir, toda la documentación de apoyo como las ejecuciones del control.

Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar.

El sistema de gestión de seguridad de la información se fundamenta en 3 pilares fundamentales, preservar la confidencialidad, la integridad y la disponibilidad de la información (Ver figura N° 6).

Figura N° 6 Pilares de la Seguridad de la Información
Fuente: http://seguinfo2012.blogspot.com/p/imagenes-del-tema.html

2.1.2. ISO/IEC 27001: 2005

ISO/IEC 27001 (2005) “Este Estándar Internacional adopta el modelo del proceso Plan-Do-Check-Act (PDCA) también llamado Ciclo de Deming, el cual se puede aplicar a todos los procesos del sistema de gestión de seguridad de la información. Este modelo tiene una serie de fases y acciones que establecen un modelo de indicadores y métricas comparable en el tiempo.” (p. 18)

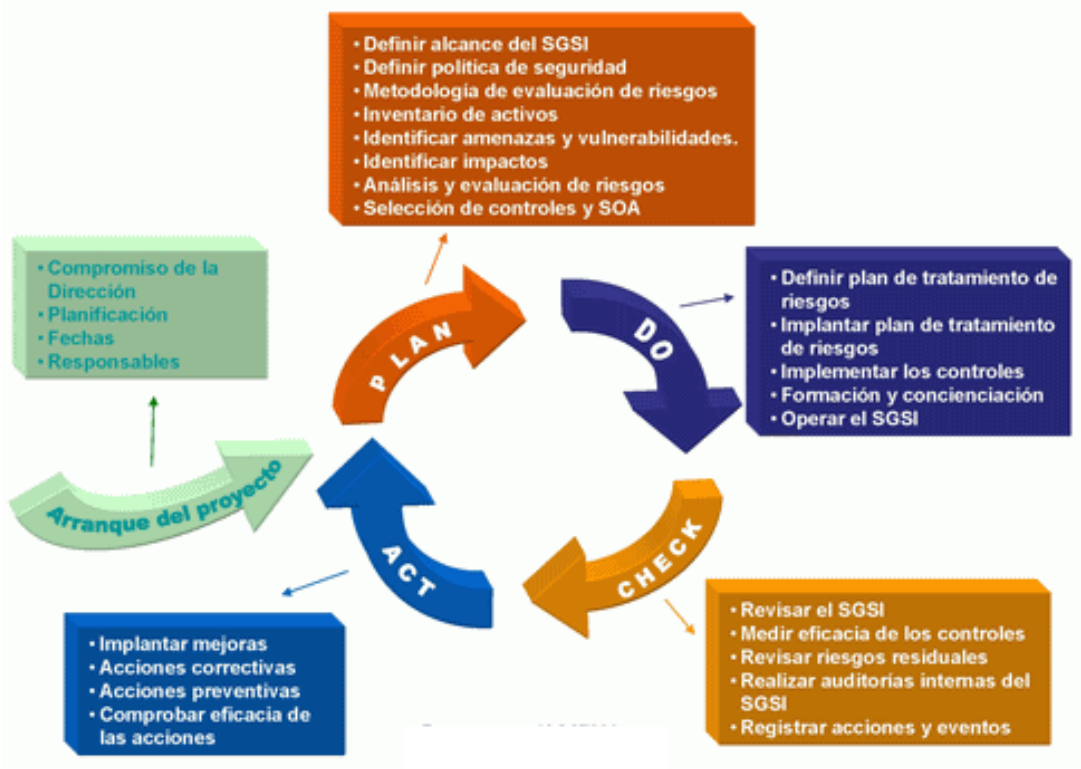


Figura N° 7 Ciclo de Deming
Fuente: https://ingenioempresa.com/ciclo-pdca/

Cada fase es parte de un ciclo (Ver figura N° 7), a continuación se detalla una descripción de cada fase:

- Planear (Establecer el SGSI)
  - En esta fase se planifican y diseñan los objetivos, políticas, procesos y procedimientos.
  - Se determina el alcance para la implementación, medios que se utilizará, los procesos del negocio involucrados y los activos que lo soportan.
  - Identifica, evalúa y gestiona los riesgos de llevar a cabo los objetivos que se ha planteado.

- Se debe obtener el apoyo de la alta dirección
- Se define la política general de seguridad de información.

- Hacer (implementar y gestionar el SGSI)
  - En esta fase se define, implementa y gestiona el SGSI de acuerdo a su política, controles, procesos y procedimientos.
  - Se implementa un programa de capacitación.
  - Se implementa el plan de tratamiento al riesgo.
- Chequear (monitorizar y revisar el SGSI)
  - En esta fase se verifica, mide y revisa los procesos del SGSI.
  - Se comprueba que las medidas que se adoptaron han surtido efecto, para ello se vuelven a recopilar datos y se monitorea el comportamiento del sistema.
  - Se realizan periódicamente las auditorías internas del SGSI en intervalos planificados.
- Actuar (mantener y mejorar el SGSI)
  - En esta fase se aplican las acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI.
  - Se comunican las acciones y mejoras a las partes interesadas.

2.1.3. Sistemas de Gestión de la S.I. - Requisitos ISO/IEC 27001: 2013

ISO/IEC 27001 (2013) “Esta Norma internacional define los requisitos para para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información dentro del contexto de la organización.” (p. 41)

Cabe recalcar que el sistema de gestión de seguridad de la información necesita formar parte y se necesita integrar con los procesos y las estructuras de gestión integral de la organización.

Esta norma internacional incluye los requisitos para la evaluación y el tratamiento de los riesgos de la información que están adaptados a las necesidades de la organización (Ver figura N°8). Los requisitos de esta Norma Internacional son genéricos y se elaboraron para aplicarlos en todas las organizaciones, independientemente de su naturaleza, tamaño y tipo.

Esta norma internacional estipula 10 cláusulas de las cuales las secciones de 1 a 3 son introductorias y las secciones de 4 a la 10 son obligatorias, esto significa que para que la organización cumpla con la norma, sebe cumplir con los requerimientos de esas secciones.

Figura N° 8 Normativa según la ISO 27000
Fuente: https://steadulenam.ml/iso-270012013-dominios-de-control-de-objetivos-y-controles

Descripción breve de las secciones:

1. Alcance: Establece la obligatoriedad del cumplimiento de los requisitos de las secciones.
2. Referencias normativas: Constituyen referencias normativas de la ISO 27001.

3. Términos y definiciones: Son los términos y definiciones utilizados en la ISO/IEC 27000.
4. Contexto de la organización: Determina los asuntos internos y externos que son importantes para sus objetivos, también define las partes interesadas que son relevantes, los requisitos y el alcance del SGSI.
5. Liderazgo: La Alta Dirección debe demostrar liderazgo y comprometerse con el SGSI.
6. Planificación: Define los requisitos para la evaluación de riesgos de la seguridad de la información, los criterios, la identificación y el tratamiento de ellos.
7. Soporte: Define los recursos, competencias, concienciación, comunicación.
8. Operación: Define la planificación, implementación y control de los procesos para cumplir con los requerimientos de la seguridad de la información.
9. Evaluación del desempeño: La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la información.
10. Mejora: Define los requerimientos para el tratamiento de no conformidades, las acciones correctivas.

2.1.4. Tecnología workflow

García Moreno M. (1999) define el término workflow como:

> Workflow o Flujos de trabajo es una combinación de las reglas de negocio y mecanismos que permiten la automatización y gestión de procesos a través del movimiento inteligente de información. El workflow se encarga de la circulación de la información electrónica, datos y documentos en cualquier aplicación, así como la ejecución de una serie de tareas y de los plazos para su ejecución. (p. 25)

Tipos de workflow

- Workflow de Producción
- Workflow de Colaboración
- Workflow Administrativo
- Workflow Ad Hoc

Herramientas: Las herramientas de análisis son programas que permiten la representación gráfica del proceso, permite la generación de informes y gráficos. La herramienta comprueba que el proceso que se definió se comporta según lo esperado.

2.1.5. Ciclo de Deming

Cuatrecasas (2010) define el ciclo de Deming como:

> Ciclo de mejora, actúa como guía para llevar a cabo la mejora continua y lograra una forma sistemática y estructurada la resolución de problemas. Está constituido específicamente por cuatro actividades: planear, realizar, verificar y actuar, formar un ciclo que se repita de forma continua. También se conoce como ciclo PDCA, siglas en inglés de Plan, Do, Check, Act. (p 37)

Dentro de este libro que abarca los conceptos y metodologías de la gestión de la calidad, también mencionan el ciclo de Deming (Ver Figura N° 9) ya que es parte de la mejora continua y nos ayuda a utilizar la lógica para diversas situaciones o actividades, con ello se logra comprender la importancia de estas fases y ello nos sirvió de input para la realización de nuestros casos de uso.

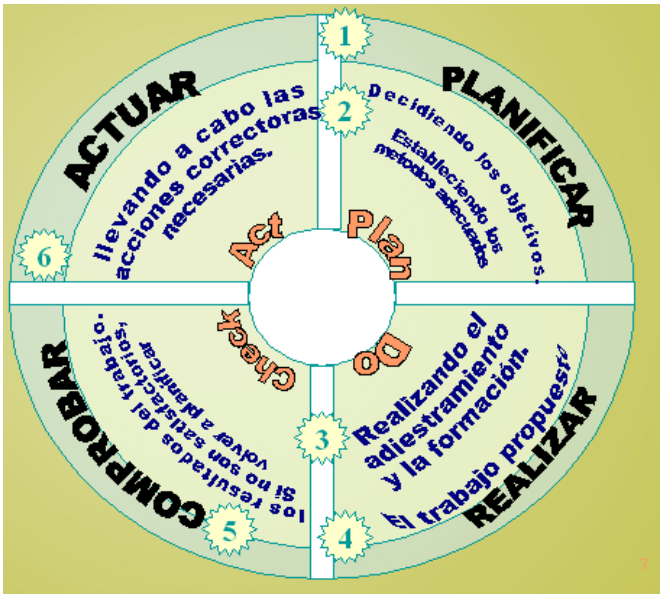


Figura N° 9: Rueda de Deming
Fuente: https://www.monografias.com/trabajos105/ciclo-mejora-continua-pdca/ciclo-mejora-continua-pdca.shtml

2.2. Estado del arte

2.2.1. Trabajos realizados (Investigación y Software)

2.2.1.1. Heurísticas para evaluar herramientas de gestión de seguridad de TI.

Jaferian, Hawkey, Sotirakopoulos, Velez-Rojas, & Beznosov (2011)

> Las empresas son cada vez más sujeto a las normas de cumplimiento que se originan en las directrices corporativas, las normas del sector de la industria, y las leyes. El objetivo del control de acceso es para proteger contra usuarios no autorizados. Sin embargo, las amenazas a menudo residen dentro de las organizaciones donde los usuarios autorizados pueden emplear mal los recursos del sistema. Aunque el control de acceso es fundamental en la protección de los sistemas de información, que puede suponer un obstáculo para el logro de los objetivos de negocio. Hoy en día, las políticas de seguridad tienen que estar alineados con los objetivos de negocio y no son más una cuestión puramente técnica. (p. 53)

Utilidad:

Gracias a este trabajo de investigación se tiene una mejor visión de las heurísticas de la administración de Seguridad de la información, además de los procesos de las organizaciones, para tener un panorama del cumplimiento de la seguridad en el área de TI.

2.2.1.2. Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A

Saberi, Federrath, & Shojaie (2014)

> La parte del sistema de gestión de una organización que trata con seguridad de la información se denomina Sistema de Gestión de Seguridad de la Información (SGSI). El estándar SGSI más adoptada es la norma ISO 27001: 2005. La versión 2005 de la norma se ha actualizado en 2013 para proporcionar más claridad y más libertad en la ejecución, sobre la base de experiencias prácticas. Este trabajo compara la norma ISO 27001: 2005 y la norma actualiza 2013, basado en los controles del Anexo A. Clasificamos los controles en cinco categorías: de datos, hardware, software, personas y red.

> Todos los controles definidos en el Anexo A, independientemente de sus objetivos, puede ser fácilmente asignados a al menos una de estas categorías. La clasificación de los controles a las categorías conocidas ofrece una visión integrada de la norma actualizada y presenta una guía adecuada para evaluar el rendimiento y la eficiencia de la norma actualizada. (p. 25)

Utilidad:

Gracias a este artículo se conocen los parámetros de la norma ISO 27000, y su gran ayuda en la seguridad de la información.

2.2.2. Trabajos realizados (Software)

2.2.2.1. Global Suite

Figura N° 10 Logo del Software "Globalsuite"
Fuente: (Globalsuite, 2016)

Global suite (ver figura N° 10), es un software para la gestión y mantenimiento de sistema de gestión de seguridad de información, fácil de usar e intuitiva.

Las características que tiene son las siguientes:

Identificación de Riesgos

Orientación de servicio y procesos a través del inventario de activos. Configuración de las dimensiones y niveles de valoración.

Análisis de Riesgos

Parametrización de probabilidad e impacto, valoración de riesgos, análisis de costes, amenazas por activos y configurables.

Evaluación de Riesgos

Definición de riesgo aceptable, niveles de riesgo aceptable, listado de riesgos, mapa de riesgos, riesgos simultáneos o dependientes.

Gestión de Riesgos

Catálogo de controles configurables y resumen de los mismos, Parametrización de la gestión, reevaluación del riesgo, cuestionarios parametrizables (Ver figura N° 11).

Figura N° 11 Medición de riesgos según el Software “globalsuite”
Fuente: https://www.globalsuitesolutions.com/es/

Procesos SGSI

Permite gestionar la propuesta de indicadores, Análisis Diferencial, Declaración de Aplicabilidad, gestión de la capacidad, gestión de cambios y adquisiciones, etc.

Gestor Documental

Posibilita el control de toda la documentación, en distintos formatos y con control de versiones, para que sirva de apoyo en la gestión integral de la seguridad de su organización.

Planes de Continuidad, Capacidad y Formación

Permite realizar un historial de cada uno de los planes y asignar métricas para su seguimiento.

Actas de reunión

Posibilita el registro de acciones del comité de seguridad, envío automático de actas a los asistentes por mail y guardado automático de los documentos.

Utilidad en la tesis

Gracias a este software se tuvo un panorama más amplio acerca de los procesos que debe contener el SGSI, y nos ayudó en la generación de reportes para el monitoreo de los planes de capacitación.

2.2.2.2. Sistema "Meycor"

Figura N° 12 Logo del Software "Meycor"
Fuente: (meycor, 2015)

El sistema "Meycor" (Ver Figura N° 12) permite el desarrollo, la implantación y mantenimiento de sistemas de gestión ISO. Incluye un módulo de políticas y procedimientos. Permite el registro de incidentes y eventos.

El software se diseñó para simplificar la implementación y el mantenimiento de cualquier tipo de sistema que implique requisitos de gestión documental y de eventos.

Central

Este módulo permite la administración de usuarios, grupos, eventos, generación de novedades, visualización de logs y configuración de aspectos más técnicos del producto (Ver Figura N°13).

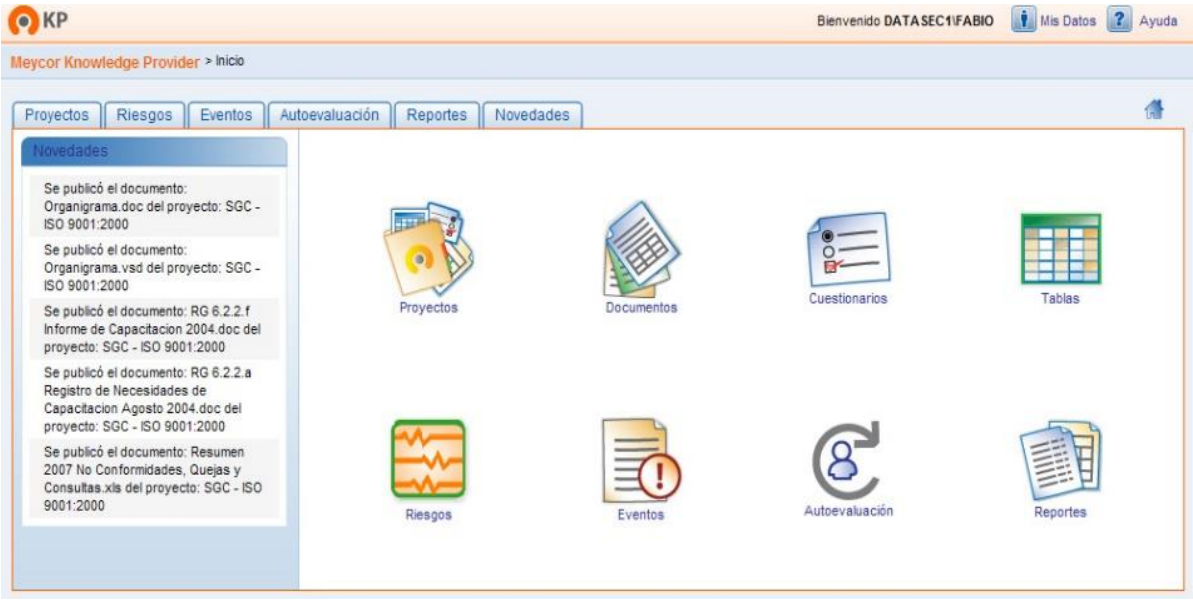


Figura N° 13 Pantalla principal de acceso al software

Fuente: (meycor, 2015)

Gestión documental

Este módulo permite la administración de documentos y cuestionarios, pudiendo mantener un control sobre las transiciones entre los estados en que estos se puedan encontrar a lo largo de su ciclo de vida (Ver Figura N°14). Los documentos pueden ser desarrollados directamente en el módulo, sin importar su formato.

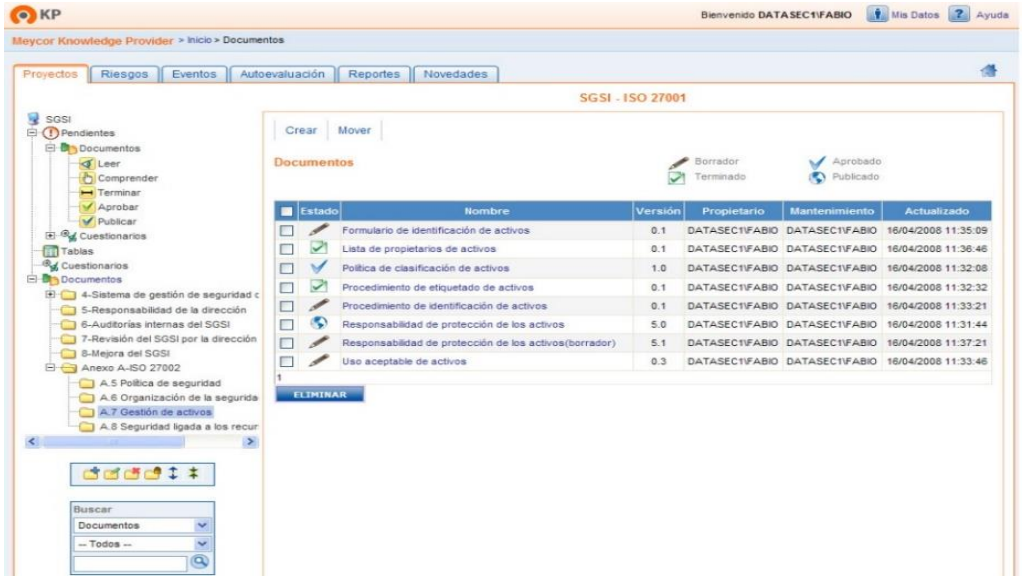


Figura N° 14 Módulo “Gestión documental”

Fuente: (meycor, 2015)

Gestión de riesgos

Este módulo permite la gestión y seguimiento de Análisis de Riesgos. Es posible la identificación de activos, amenazas y vulnerabilidades, generándose resultados de riesgo actual y residual. Se incluyen los objetivos y controles de la ISO/IEC 27002 para facilitar el tratamiento de riesgos (Ver Figura N° 15). Incluye, a su vez, la generación del Enunciado de Aplicabilidad de Controles y Planes de Tratamiento

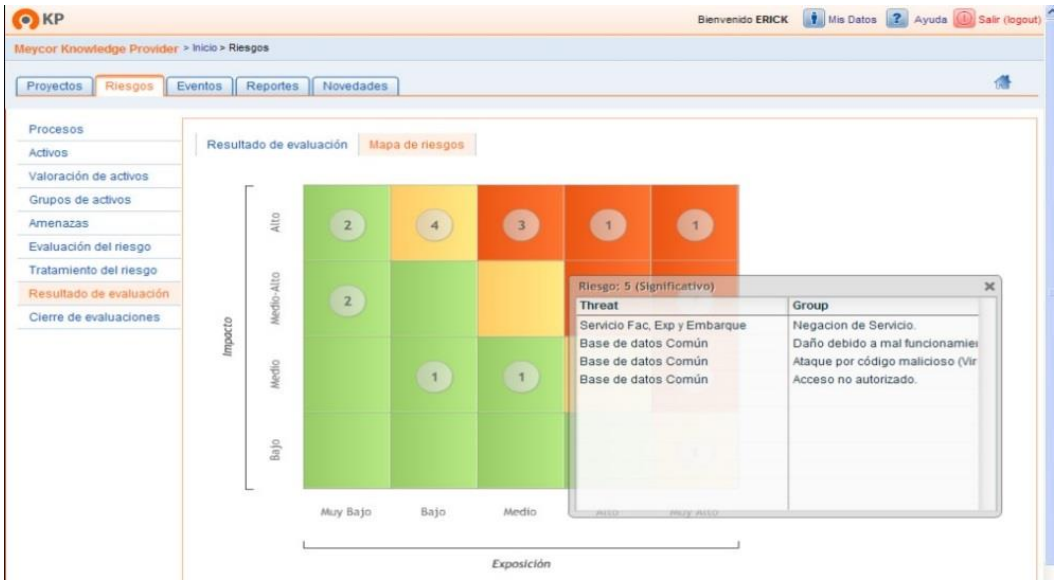


Figura N° 15 Módulo "Gestión de riesgo
Fuente: (meycor, 2015)

Gestión de eventos

Este módulo permite gestionar y definir workflows de diferentes tipos y lógica de eventos. Por medio de este módulo es posible manejar: Eventos de Seguridad, No Conformidades, Acciones Correctivas y Preventivas, Solicitudes de Cambios y muchos más.

Auto-evaluación de controles

Este módulo permite a las organizaciones autoevaluarse contra distintas buenas prácticas como ser: ISO/IEC 27002, ISO/IEC 20000, COBIT, COSO I, COSO II y cualquier otro marco de evaluación que la organización desee utilizar.

Comunicaciones

Este módulo permite generar alertas que son enviadas por e-mail a los usuarios involucrados en diferentes situaciones configurables. Algunos casos de ejemplo son:

cuando un documento debe ser aprobado o publicado, cuando un documento llega a su vencimiento, cuando debe ser tratado algún evento reportado, y muchos más.

Utilidad en la tesis

Gracias a este sistema se podrá adicionar la gestión de documentos en el que permitirá un control sobre los cambios de estos y mantener la administración de los estados de los documentos a lo largo de su desarrollo, logrando ver las fechas de las modificaciones, a cargo de quién, la versión del documento y gracias a esto se podrán ver un histórico de los cambios realizados.

2.2.2.3. Sistema "Novasec"

Figura N° 16 Logo del Software "Novasec"
Fuente: (NovaSec, 2015)

El software NovaSec MS (Ver Figura N°16) es una suite de soluciones, que permite a las empresas manejar vía web la información y los reportes relacionados la gestión de los riesgos, el cumplimiento normativo, los incidentes, los indicadores, la seguridad de la información, la continuidad del negocio y la mejora continua de sus sistemas de gestión.

Está compuesto por los módulos Administración, Gestión y Reportes.

Características de sistema en el control de Activos:

Módulo Administración:

- Permite define la escala de valoración que se va a utilizar para medir el impacto, la probabilidad y los niveles de riesgos que va a tener la matriz, así como los colores que representan cada nivel y personalizar la descripción de las escalas definidas.
- Establecer cuales recursos del negocio van a ser considerados dentro del cálculo del impacto de los riesgos.

Módulo Gestión:

- Registrar la información de la identificación del riesgo.
- Realizar la valoración de los riesgos sobre los activos o sobre los proceso, el impacto sobre los recursos, obteniendo automáticamente los niveles de riesgo que se hayan configurado en la metodología.

Módulo Reportes:

- Consultar riesgos específicos consultando por diversos criterios que permiten tomar decisiones y entender mejor la naturaleza de los riesgos.

Obtener reportes de datos y gráficos acerca de:

- Top de vulnerabilidades, amenazas o factores y causas o activos con mayores cantidades de riesgos.

Características de sistema en el control de Riesgos:

Módulo Administración

- Define las escalas de valoración que se van a utilizar para medir el impacto, la probabilidad y los niveles de riesgos que va a tener la matriz, así como los colores que representan los niveles de riesgos y personalizar la descripción de estas escalas de valoración.
- Establece cuales recursos del negocio van a ser considerados dentro del cálculo del impacto de los riesgos (Recursos: financiero, operación, imagen, legal, ambiental, personas, etc.)

Módulo Gestión:

- Registra la información de la identificación del riesgo, con su nombre, descripción, clase, amenazas, vulnerabilidades (ISO 27005) o Factores y causas de riesgo (ISO 31000), controles existentes, observaciones, entre otros.
- Realiza la valoración de los riesgos sobre los activos o sobre los procesos determinando la probabilidad de ocurrencia, el impacto sobre los recursos del negocio, obteniendo automáticamente los niveles de riesgo que se hayan configurado en la metodología.

Módulo Reportes:

- Consulta riesgos específicos consultando por diversos criterios que permiten tomar decisiones y entender mejor la naturaleza de los riesgos.

- Top de vulnerabilidades, amenazas o factores y causas o activos con mayores cantidades de riesgos.

Características de sistema en el control de Normatividad:

Módulo Administración

- Permite cargar y administrar las normas, estándares o leyes que se requieren tener en el sistema para realizar tratamiento de activos, riesgos y análisis de cumplimiento.
- Define el alcance de aplicación de cada norma.

Módulo Gestión:

- Registra toda la información de los hallazgos producto de auditorías internas o externas, clasificarlos y definir fechas de cierre.
- Hace el análisis de causas y consecuencias de los hallazgos.

Módulo Reportes:

- Estado de los hallazgos.
- Genera reportes a través de criterios de filtros y selección de información de los hallazgos a través de un generador dinámico de reportes.

Características de sistema en el control de Incidentes:

Módulo Administración

- Define las escalas de valoración que se van a utilizar para medir la criticidad, tiempos de respuesta y priorización de los incidentes y personalizar la descripción de estas escalas de valoración.
- Define los tipos de incidentes y eventos que se van a manejar en el proceso de gestión de incidentes.

Módulo Gestión:

- Permite que los usuarios reporten los eventos de seguridad en el sistema.
- Administra la información del proceso de identificación, valoración y tratamiento de los incidentes, seleccionando los activos afectados y los riesgos que se materializan por el incidente.

Módulo Reportes:

Obtiene los reportes de la gestión de incidentes en cuanto:

- Motor de búsqueda de incidentes.
- Histórico de incidentes.

Características de sistema en el control de Indicadores:

Módulo Administración

- Administrar los atributos, los roles, las medidas base, escalas, unidades de medición, frecuencias de medición y otras variables para la definición y valoración de los indicadores.
- Definir los periodos sobre los cuales se va a realizar la medición, revisión y reporte de los indicadores.

Módulo Gestión:

- Calificar el nivel de cumplimiento de los indicadores.
- Permitir que los usuarios gestionen la información de los indicadores y se adicione información de seguimiento.

Módulo Reportes:

- Obtener los reportes de la gestión de indicadores en cuanto:
- Gráficas de resultados de la medición de indicadores.
- Hoja de vida de los indicadores.

Características de sistema en el control de Continuidad:

Módulo Administración

- Definir los impactos y los niveles con los cuales se van a medir los mismos.
- Establecer la metodología de valoración de impactos al negocio y rangos de valoración.

Módulo Gestión:

- Llevar un registro de interrupciones ocurridas.
- Registrar los periodos críticos de operación

Módulo Reportes:

- Obtener el informe general de BIA con impactos, variables, periodos críticos, recursos, etc.

- Generar sus propios reportes aplicando diferentes criterios de filtrado y selección de información a través de un generador dinámico de reportes.

Características de sistema en el control de Eventos:

Módulo Administración:

- Definición de los tipos de eventos que se manejarán en el sistema.

Módulo Gestión:

- El sistema permite que los usuarios puedan reportar eventos de los diferentes sistemas de gestión empresariales incluyendo eventos de pérdida para riesgos operativos.
- Realizar la identificación del evento con su tipo, nombre, descripción, impacto, estado, fechas, calificación y localización.

Módulo Reportes:

- Generador dinámico de reportes que permite filtrar la información de los eventos para poder obtener los eventos de interés. Estos reportes se pueden exportar.

Utilidad en la tesis

Gracias a este sistema se podrá adicionar reportes de datos y gráficos de acuerdo a los criterios que queramos, también reportes comparativos en diferentes periodos en el que se podrá obtener estadísticas mensuales o por un determinado periodo de tiempo que requiramos.

2.2.3. Benchmarking

Benchmarking con puntaje para el "Sistema de Gestión de Seguridad de una Empresa basado en la Norma ISO 27001"									
Análisis Comparativo		GLOBAL SGSI http://www.globalsgsi.com/es/productos-globalsuite/globalsgsi.html		MEYCOR KP http://www.meycor-soft.com/es/meycor-kp		NOVASEC MS http://www.novasec.co/soluciones/novasec-ms/normatividad		SISTEMA PROPUESTO	
Aspectos Funcionales	Peso	Funcionalidad	Valor	Funcionalidad	Valor	Funcionalidad	Valor	Funcionalidad	Valor
Calificar el nivel de cumplimiento de los controles	3	2	6	2	6	3	9	3	9
Facilidad de uso	2	3	6	2	4	2	4	3	6
Mantenimiento	2	1	2	2	4	2	4	3	6
Envío de Acciones correctivas	3	3	9	3	9	2	6	3	9
Permitir que los usuarios justifiquen la calificación de cumplimiento	2	1	2	0	0	3	6	3	6
Definir tiempos para el cumplimiento	2	0	0	2	4	3	6	3	6
Permite administrar usuarios	1	0	0	3	3	0	0	3	3
Guardar los registros de información y evidencia	3	3	9	3	9	2	6	3	9
Permite gestionar cada dominio	3	2	6	1	3	3	9	3	9
Permite emitir informes	3	2	6	2	6	3	9	3	9
TOTAL DEL PUNTAJE			46		48		59		72
Software Base									
Sistema Operativo		Windows 7		Windows 7		Windows 7		Windows 7	
Servidor de Base de Datos		No muestra		No muestra		No muestra		SQL Server 2008 R2	
Lenguaje de Programación		No muestra		No muestra		No muestra			
Automatización de procesos									
Configuración									
Procesador								Intel dual-core de 1.2GHz	
Memoria								2GB interno	

Leyenda de Funcionalidades	Peso
0 = No tiene esta funcionalidad	1 = No muy importante
1 = Baja (poco amigable y pocos datos)	2 = Importante
2 = Media (poco amigable o con datos insuficientes)	3 = Muy importante
3 = Alta (amigable y con datos suficientes)	

Figura N° 17 Cuadro comparativo (benchmarking).
Fuente: Elaboración propia

Se ha realizado la comparación del sistema con otros 3 sistemas de similar implementación, del cual el sistema SGSI obtuvo el mayor porcentaje (Ver Figura N° 17).

2.2.4. Herramientas para la implementación

Para el desarrollo de la solución se han considerado diferentes herramientas de programación, base de datos y frameworks.

Se empleó los siguientes:

- Base de datos : Microsoft SQL Server 2014
- Programa para el desarrollo y automatización de los procesos: Bizagi Studio
- Framework: .NET Framework versión 4.6.1

2.2.5. Definición de términos

- **Activo tecnológico**: Son los bienes materiales que posee la empresa como por ejemplo las computadoras.
- **Activo de Información:** Son los datos relevantes que posee una empresa como por ejemplo la información guardada dentro de las BDD.
- **Bitácora**: es un archivo en el cual se lleva un registro periódicamente de la tarea que se realiza en los equipos
- **GSI**: Significa Gestión de seguridad de la información.
- **IEC**: Comisión Electrotécnica Internacional es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.
- **ISO**: Organización Internacional para la Estandarización es el organismo encargado de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones.
- **ISO 27001:** Es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa.
- **Mejora continua:** Es una de las ventajas que trae consigo la implementación de la ISO 27001 la cual permite un crecimiento y optimización de factores importantes de la empresa en este caso la gestión de la seguridad.
- **Medios Removibles:** Son unidades de almacenamiento portales que sirven para poder llevar la información de un lugar a otra de manera ligera.

- **Normalización:** Es el proceso de formulación, elaboración, la aplicación y mejoramiento de las normas existentes que se aplican a las diversas actividades económicas con el objetivo de ordenarlas y mejorarlas.
- **Plan de contingencia:** es utilizado únicamente cuando ya se ha caído en un desastre, solución al problema presentado.
- **Plan de Continuidad:** A parte de tener medidas en caso de desastre también analiza las vulnerabilidades y desarrolla contramedidas para mitigar dichas vulnerabilidades.
- **SGSI**: Significa sistema de gestión de la seguridad de la información que son un conjunto de políticas de administración de la información.
- **TI**: Significa tecnología de la información y hace referencia al uso tecnologías para el manejo y procesamiento de la información.

CAPÍTULO 3: DESARROLLO DEL PROYECTO

3.1. Alcance del proyecto

3.1.1. Estructura del desglose del trabajo y entregables

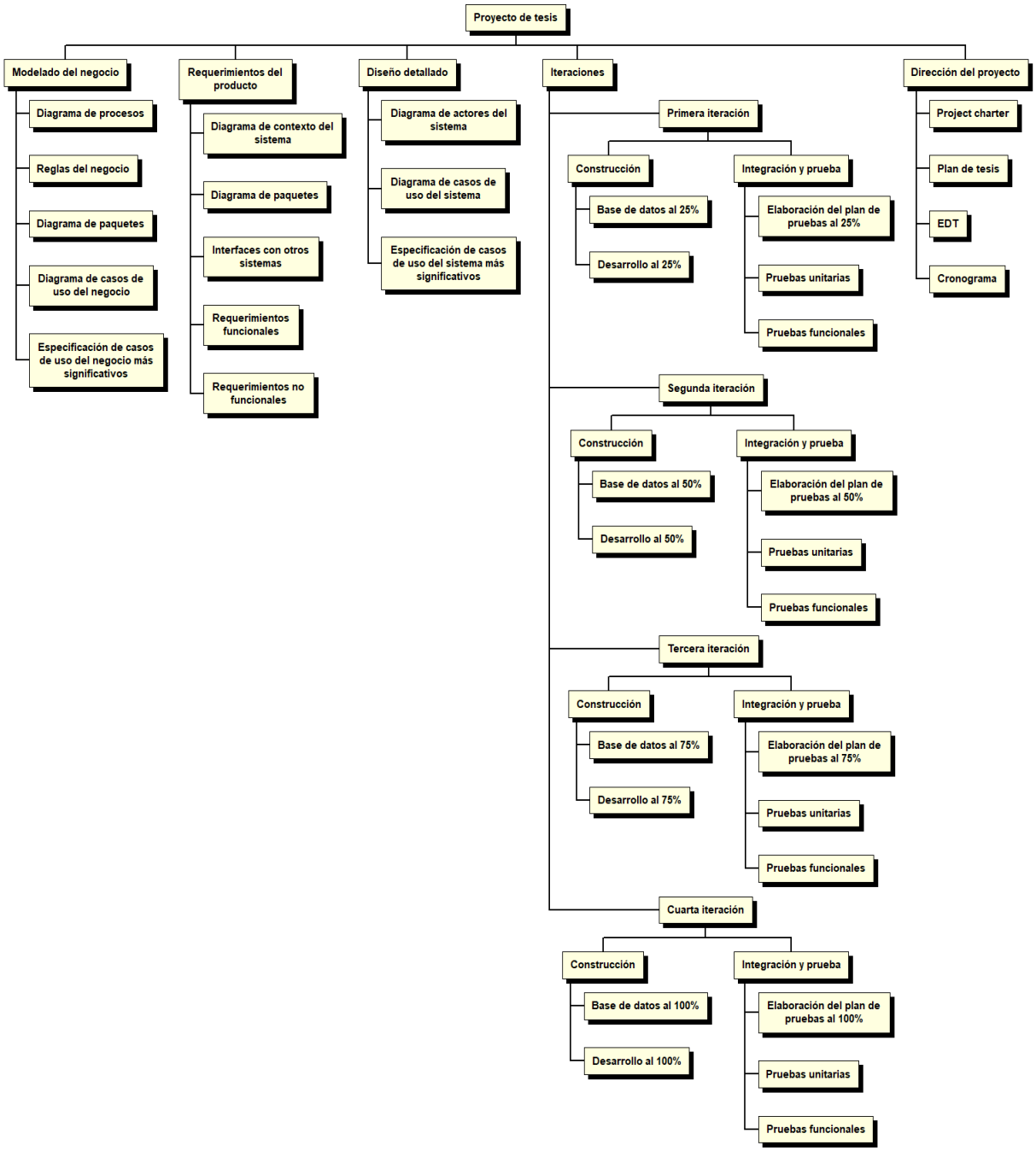


Figura N° 18 EDT
Fuente: Elaboración propia

En el EDT se muestran los módulos de trabajo que fueron ejecutados por el equipo del proyecto, el que se utilizó para la definición del alcance del proyecto de tesis, que tiene como objetivo es conocer los entregables por semana y el seguimiento del cronograma (ver figura N ° 18).

3.1.2. Exclusiones del proyecto

- No se contempla la implementación y certificación de la ISO 27001
- Monitoreo de todos los controles.
- Análisis de gestión de riesgo de la empresa.
- Gestión y seguimiento de incidentes.

3.1.3. Restricciones del proyecto

- El máximo de usuarios que soporta Bizagi gratuitamente es de 20.
- No se permite la modificación del documento a tiempo real.
- El tiempo de duración del proyecto es de cinco (05) meses.

3.1.4. Supuestos del proyecto

- Para que se tenga resultado satisfactorio, los colaboradores deben estar capacitados sobre la ISO 27001.
- La alta dirección debe mostrar compromiso, garantizando el establecimiento de la política y objetivos de la seguridad de la información.
- El sponsor nos facilite de forma inmediata la información requerida.

3.1.5. Cronograma del proyecto

Se ha realizado el cronograma para la realización del proyecto.

Tabla 2: Cronograma general

Modo de	Nombre de tarea	Duración	Comienzo	Fin
	FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
	1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
	2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
	3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
	4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
	0.0 Gestión de Proyectos	**25 días**	**vie 14/06/19**	**mar 9/07/19**

Fuente: Elaboración propia.

El cronograma general con los módulos realizados en el proyecto de tesis y sus respectivas fechas de presentación y término de actividades (Ver tabla 2).

Tabla 3: Modelado de Negocio

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
1.1 Diagrama de Procesos	3 horas	dom 12/05/19	dom 12/05/19
1.2 Reglas de Negocio	8 horas	dom 12/05/19	lun 13/05/19
1.3 Diagrama de Paquetes del Negocio	2 horas	lun 13/05/19	lun 13/05/19
1.4 Diagramas de casos de uso del Negocio	5 horas	lun 13/05/19	lun 13/05/19
1.5 Especificaciones de casos de uso mas significativos	10 horas	lun 13/05/19	mar 14/05/19
Aprobación de documentación de modelado del Negocio	0 días	mar 14/05/19	mar 14/05/19

Fuente: Elaboración propia

En el módulo de “Modelado de negocio” se presentan las actividades realizadas en el proyecto de tesis con sus respectivas fechas de presentación (Ver tabla 3).

Tabla 4: Requerimiento del Producto

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
2.1 Diagramas del Sistema	5 horas	mar 14/05/19	mié 15/05/19
2.2 Interfaces con otros sistemas	10 horas	mié 15/05/19	jue 16/05/19
2.3 Requerimientos Funcionales	1 día	jue 16/05/19	vie 17/05/19
2.4 Requerimientos no Funcionales	4 días	vie 17/05/19	mar 21/05/19
Aprobación de documento de requerimiento del producto	0 días	mar 21/05/19	mar 21/05/19

Fuente: Elaboración propia.

En el módulo de “Requerimientos del producto” se presentan las actividades realizadas para la entrega del sistema final (Ver tabla 4).

Tabla 5: Diseño detallado

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
3.1 Diagrama de Estructura	**10 días**	**mar 21/05/19**	**vie 31/05/19**
Diagrama de Clases	2 días	mar 21/05/19	jue 23/05/19
Diagrama de Componentes	2 días	jue 23/05/19	sáb 25/05/19
Diagrama de Objetos	2 días	sáb 25/05/19	lun 27/05/19
Diagrama de Despliegue	2 días	lun 27/05/19	mié 29/05/19
Diagrama de Paquetes	2 días	mié 29/05/19	vie 31/05/19
3.2 Diagrama de Comportamiento	**9 días**	**vie 31/05/19**	**dom 9/06/19**
Diagrama de Estados	3 días	vie 31/05/19	lun 3/06/19
Diagrama de Actividades	3 días	lun 3/06/19	jue 6/06/19
Diagrama de Casos de Uso del Sistema	2 días	jue 6/06/19	sáb 8/06/19
Diagrama de Actores del Sistema	1 día	sáb 8/06/19	dom 9/06/19
3.3 Diagrama de Interacción	**5 días**	**dom 9/06/19**	**vie 14/06/19**

Fuente: Elaboración propia

En el módulo de “Diseño detallado” se presentan las actividades realizadas en el proyecto de tesis con sus respectivas fechas (Ver tabla 5). Cada diagrama realizado se realizó en el software rational rose.

Tabla 6: Primera iteración

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
4.1 Primera Iteración	**56 días**	**sáb 15/06/19**	**vie 9/08/19**
4.1.1 Construcción	**18 días**	**sáb 15/06/19**	**mar 2/07/19**
Base de Datos al 25%	18 días	sáb 15/06/19	mar 2/07/19
4.1.2 Desarrollo al 25%	**36 días**	**mié 3/07/19**	**mié 7/08/19**
Construcción del caso aprobar documentación	9 días	mié 3/07/19	jue 11/07/19
Construcción del caso de uso Comunicar actualizacione	8 días	vie 12/07/19	vie 19/07/19
Construcción del caso de uso definir metodología de ri	9 días	sáb 20/07/19	dom 28/07/19
Construcción del caso de uso gestionar evidencia	3 días	lun 29/07/19	mié 31/07/19
Construcción del caso de uso gestionar plantilla	2 días	jue 1/08/19	vie 2/08/19
Construcción del caso de uso programar capacitación c	3 días	sáb 3/08/19	lun 5/08/19
Construcción del caso de uso Revisar documentación	2 días	mar 6/08/19	mié 7/08/19
Aprobación de Modulos al 25%	0 días	mié 7/08/19	mié 7/08/19
4.1.3 Integración y Pruebas	**1.1 días**	**jue 8/08/19**	**vie 9/08/19**
Elaboración del plan de Pruebas al 25%	5 horas	jue 8/08/19	jue 8/08/19
Pruebas Unitarias	6 horas	jue 8/08/19	vie 9/08/19
Aprobación del plan de pruebas al 25%	0 días	vie 9/08/19	vie 9/08/19

Fuente: Elaboración propia

En el módulo de “Iteraciones” se observan las actividades realizadas en la primera iteración para el proyecto de tesis, cada actividad con su respectivas fechas de presentación (Ver tabla 6).

Tabla 7: Segunda iteración

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
4.1 Primera Iteración	**56 días**	**sáb 15/06/19**	**vie 9/08/19**
4.2 Segunda Iteración	**16 días**	**vie 9/08/19**	**sáb 24/08/19**
4.2.1 Construcción	**3 días**	**vie 9/08/19**	**lun 12/08/19**
4.2.2 Desarrollo al 50%	**8.1 días**	**vie 9/08/19**	**sáb 17/08/19**
Construcción del caso de uso Implementar política pro	2 días	lun 12/08/19	mié 14/08/19
Construcción del caso de uso Realizar plan capacitació	2 días	mié 14/08/19	vie 16/08/19
Construcción del caso de uso Subir evidencia dominio	1 día	vie 16/08/19	sáb 17/08/19
Aprobación de Modulos al 50%	0 días	vie 9/08/19	vie 9/08/19
4.2.3 Integración y Pruebas	**5 días**	**vie 9/08/19**	**mar 13/08/19**
Elaboración del plan de Pruebas al 50%	1 día	vie 9/08/19	vie 9/08/19
Pruebas Unitarias	1 día	sáb 10/08/19	sáb 10/08/19
Pruebas de Integración	3 días	dom 11/08/19	mar 13/08/19
Aprobación del plan de pruebas al 50%	0 días	mar 13/08/19	mar 13/08/19

Fuente: Elaboración propia

En el módulo de “Iteraciones” se observan las actividades realizadas en la tercera iteración para el proyecto de tesis, cada actividad con su respectivas fechas de presentación (Ver tabla 7).

Tabla 8: Tercera iteración

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
4.1 Primera Iteración	**56 días**	**sáb 15/06/19**	**vie 9/08/19**
4.2 Segunda Iteración	**16 días**	**vie 9/08/19**	**sáb 24/08/19**
4.3 Tercera Iteración	**29 días**	**dom 25/08/19**	**dom 22/09/19**
4.3.1 Construcción	**2 días**	**dom 25/08/19**	**lun 26/08/19**
Base de Datos al 75%	2 días	dom 25/08/19	lun 26/08/19
4.3.2 Desarrollo al 75%	**23 días**	**dom 25/08/19**	**lun 16/09/19**
Construcción del caso de uso Concientizar SGSI	8 días	mar 27/08/19	mar 3/09/19
Construcción del caso de uso Emitir Acta	2 días	mié 4/09/19	jue 5/09/19
Construcción del caso de uso Emitir informe	1 día	vie 6/09/19	vie 6/09/19
Construcción del caso de uso Revisar evidencia	2 días	sáb 7/09/19	dom 8/09/19
Construcción del caso de uso Generar Revisar informe	8 días	lun 9/09/19	lun 16/09/19
Aprobación de Modulos al 75%	0 días	dom 25/08/19	dom 25/08/19
4.3.3 Integración y Pruebas	**5 días**	**dom 25/08/19**	**jue 29/08/19**

Fuente: Elaboración propia

En el módulo de “Iteraciones” se observan las actividades realizadas en la tercera iteración para el proyecto de tesis, cada actividad con su respectivas fechas de presentación (Ver tabla 8).

Tabla 9: Cuarta Iteración

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
4.1 Primera Iteración	**56 días**	**sáb 15/06/19**	**vie 9/08/19**
4.2 Segunda Iteración	**16 días**	**vie 9/08/19**	**sáb 24/08/19**
4.3 Tercera Iteración	**29 días**	**dom 25/08/19**	**dom 22/09/19**
4.4 Cuarta Iteración	**31 días**	**lun 23/09/19**	**mié 23/10/19**
4.4.1 Construcción	**2 días**	**lun 23/09/19**	**mar 24/09/19**
Base de Datos al 100%	2 días	lun 23/09/19	mar 24/09/19
4.4.2 Desarrollo al 100%	**12 días**	**lun 23/09/19**	**vie 4/10/19**
Construcción del caso de uso Gestionar usuario	7 días	mié 25/09/19	mar 1/10/19
Construcción del caso de uso implementar medidas co	3 días	mié 2/10/19	vie 4/10/19
Aprobación de Modulos al 100%	0 días	lun 23/09/19	lun 23/09/19
4.4.3 Integración y Pruebas	**7 días**	**lun 23/09/19**	**dom 29/09/19**
Elaboración del plan de Pruebas al 100%	1 día	lun 23/09/19	lun 23/09/19
Pruebas Unitarias	1 día	mar 24/09/19	mar 24/09/19
Pruebas de Integración	5 días	mié 25/09/19	dom 29/09/19
Aprobación del plan de pruebas al 100%	0 días	dom 29/09/19	dom 29/09/19

Fuente: Elaboración propia

En el módulo de “Iteraciones” se observan las actividades realizadas en la cuarta iteración para el proyecto de tesis, cada actividad con su respectivas fechas de presentación (Ver tabla 9).

Tabla 10: Dirección de proyectos

Nombre de tarea	Duración	Comienzo	Fin
FACILITAR EL CUMPLIMIENTO DE LA ISO 27001 MEDIANTE UNA HERRAMIENTA DE TECNOLOGÍA WORKFLOW	**166 días**	**dom 12/05/19**	**jue 24/10/19**
1.0 Modelado del Negocio	**2.8 días**	**dom 12/05/19**	**mar 14/05/19**
2.0 Requerimientos del Producto	**6.5 días**	**mar 14/05/19**	**mar 21/05/19**
3.0 Diseño Detallado	**24 días**	**mar 21/05/19**	**vie 14/06/19**
4.0 Iteraciones	**132 días**	**sáb 15/06/19**	**jue 24/10/19**
0.0 Gestión de Proyectos	**25 días**	**vie 14/06/19**	**mar 9/07/19**
0.1 Project Charter	1 día	vie 14/06/19	sáb 15/06/19
0.2 Plan de Tesis	15 días	vie 14/06/19	sáb 29/06/19
0.3 EDT	2 días	sáb 29/06/19	lun 1/07/19
0.4 Cronograma	10 días	sáb 29/06/19	mar 9/07/19

Fuente: Elaboración propia

En el módulo de “Dirección de proyectos” se observa las actividades realizadas en el presente proyecto de tesis con sus respectivas fechas de entrega (Ver tabla 10).

3.2. Alcance del producto

3.2.1. Descripción del alcance del producto

Dentro del proyecto se establece que para los 14 dominios se debe cumplir el ciclo de DEMING, sin embargo el alcance está sujeto a dos dominios (Gestión de recursos humanos y gestión de activos).

La elaboración del producto es mediante la adecuación de un workflow mediante Bizagi y el almacenamiento de datos en el motor de base de datos SQL, donde facilita la mejora de procesos para el sistema de gestión de seguridad de la información, donde se elaboramos los siguientes módulos.

a) Fase de planificación, donde se establecen los objetivos y procesos necesarios para llegar a la meta, según lo trazado.
   - Obtener apoyo de la dirección
   - Definir alcance del SGSI
   - Definir política de seguridad
   - Definir metodología de evaluación de riesgos
   - Definir declaración aplicabilidad
   - Definir plan de tratamiento de riesgos
   - Establecer mapa de procesos
   - Programa capacitación y concientización

b) Fase de implementación, donde se implementan los nuevos procesos.
   - Implementación política y procedimientos
   - Realizar operaciones de controles
   - Monitoreo y medición SGSI

c) Fase de Revisión, donde se realiza la recopilación de datos, para analizarlos y evaluar si se ha producido la mejora.
   - Realizar auditoría interna

d) Fase de mantenimiento y mejora, donde se toman en cuenta las conclusiones obtenidas en la fase de revisión, además de aplicar las nuevas mejoras se detectan los errores y se pasan a documentar como lecciones aprendidas.

- Implementar medidas correctivas

e) Elaboración de un módulo de Mantenimiento, donde se pueden modificar los perfiles según los accesos.

- Administración de usuarios y permisos.

Tabla 11: Descripción de caso de uso

Módulo	Casos de Uso	Descripción
Planificación	Aprobar documentación	Aprobación de la documentación
	Crear mapa procesos	Donde se crea el mapa de Macroprocesos a utilizar
	Definir alcance	Se define el alcance del sistema de gestión de seguridad de la información
	Definir metodología de riesgos	Se define la metodología de riesgos a utilizar
	Definir política	Se define la política de gestión de seguridad de la información y de cada uno de los controles.
	Definir responsables SGSI	Se define las responsabilidades dentro del SGSI
	Definir SOA	Define la matriz de aplicabilidad de los controles según el alcance
	Definir POA	Se define el plan anula de trabajo
	Programar capacitación	Programación de capacitaciones
	Revisar documentación	Revisión de documentos del SGSI
Implementación	Implementar política procedimiento	Implementación de las políticas y procedimientos de los controles
	Realizar plan capacitación	Hacer cumplir el plan de comunicación
	Subir evidencia dominio	Subir evidencia según los controles del SGSI
Revisión	Emitir Acta	Emitir acta de la revisión
	Emitir informe	Se emite informe de revisión
	Revisar evidencia	El auditor revisa evidencia
	Revisar informe	El RAD revisa informe emitido por auditoría
Mantenimiento y mejora	Implementar medidas correctivas	De la revisión se generan acciones correctivas
	Gestionar usuario	Gestionar permisos de usuarios

Fuente: Elaboración propia

Para la elaboración de la presente tesis se realizó cuatro módulos y casos de uso por cada módulo (Ver tabla 11).

3.2.2. Criterios de aceptación del producto

a) Que el sistema cumpla con dos dominios del anexo A de la ISO / IEC 27001:2013. Los dominios utilizados con: “A.7. Seguridad de los recursos humanos” y “A.8. Gestión de activos”.
b) El sistema cuente con las validaciones de los campos.
c) El flujo principal debe estar probado y funcionando en su totalidad.
d) La solución realizada está instalada en la universidad.

CAPÍTULO 4: DESARROLLO DEL PRODUCTO

4.1. Modelado del negocio

4.1.1. Diagramas de procesos

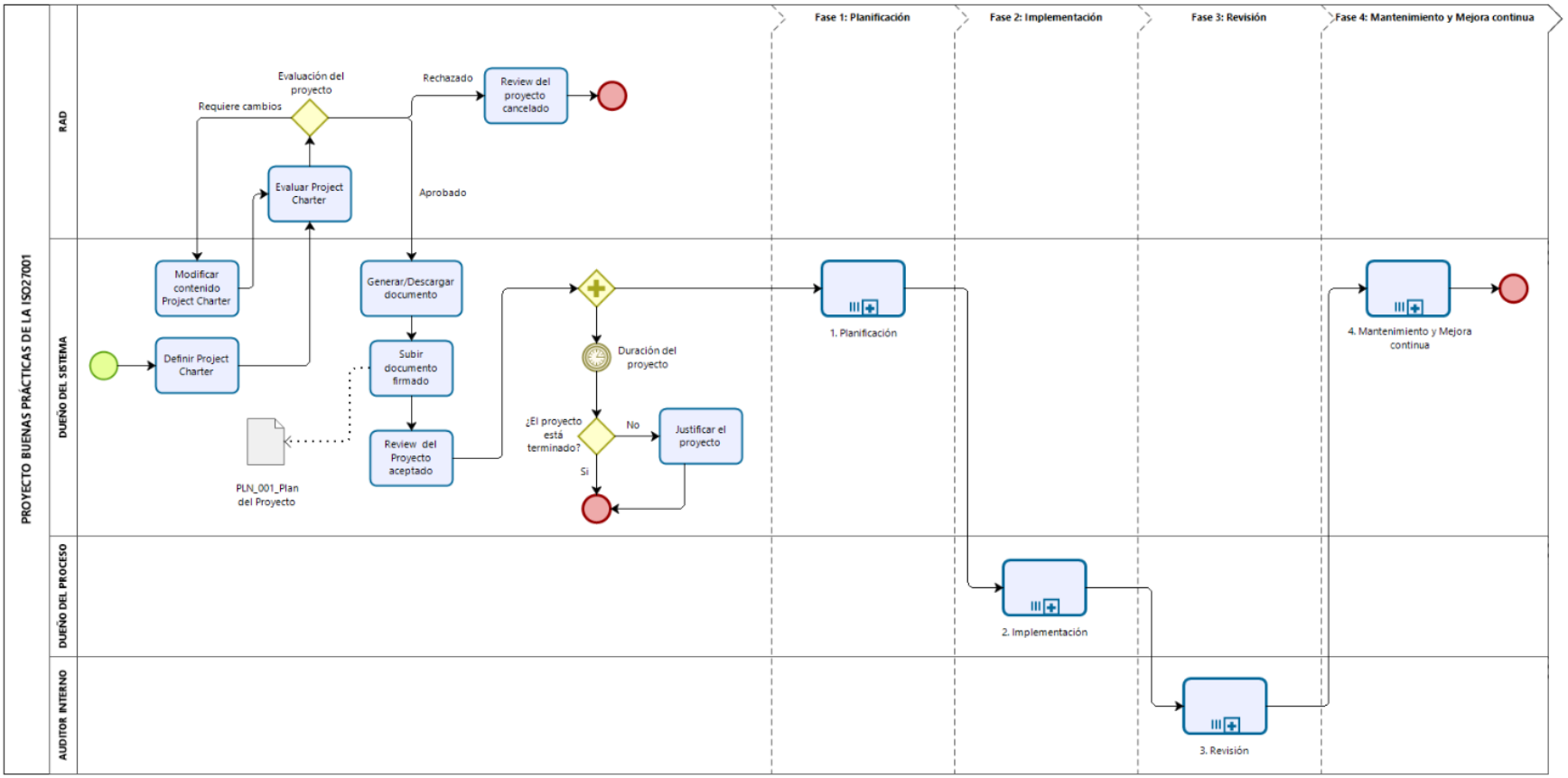


Figura N° 19 Flujo inicial - Proyecto buenas prácticas
Fuente: Elaboración propia

Los procesos del proyecto se dividieron en fases según la ISO 27001, como son la fase de planificación, implementación, revisión y mejora continua (Ver figura 19).

4.1.2. Reglas del negocio

- **RN1:** El rango de valoración de las evidencias (documentos otorgados por el jefe de área) está determinado por lo siguiente:
  a) 1-3: No conformidad
  b) 4-6: Oportunidad de mejora
  c) 6-9: Observación
  d) 10: Cumple
- **RN2:** Se debe definir fechas de corte para incluir los registros y evidencias necesarias.
- **RN3:** Solo el jefe de seguridad de TI otorga los permisos para administrar las plantillas.
- **RN4:** Toda acción correctiva debe tener su plan de tratamiento.
- **RN5**: Para pasar al siguiente módulo todo requisito debe ser evidenciado.
- **RN6**: El representante de la alta dirección debe aprobar el informe de auditoría mediante un acta de conformidad.
- **RN8**: Se necesita la autorización del jefe de área para retirar o movilizar los bienes de la organización.
- **RN9**: Manejar, operar, conducir y/o retirar de las instalaciones de la organización, equipos ajenos a la gestión de estos, salvo autorización expresa.
- **RN10**: Los colaboradores de la organización deben conocer sus funciones y responsabilidades.
- **RN11**: El jefe de área de la organización otorga las evidencias (las plantillas llenas).

4.1.3. Diagrama de paquetes

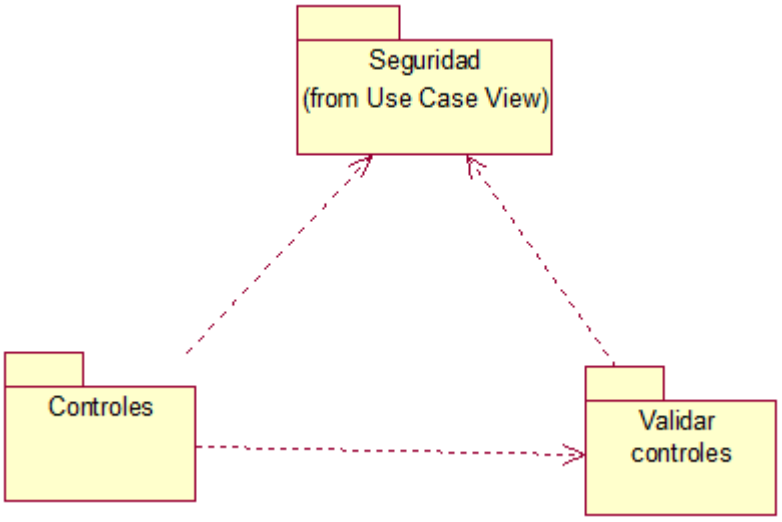


Figura N° 20 Diagrama de paquetes
Fuente: Elaboración propia

En el diagrama se muestra la relación de los paquetes del negocio que maneja industrias Triveca (Ver Figura N° 20).

4.1.4. Diagrama de caso de uso del negocio

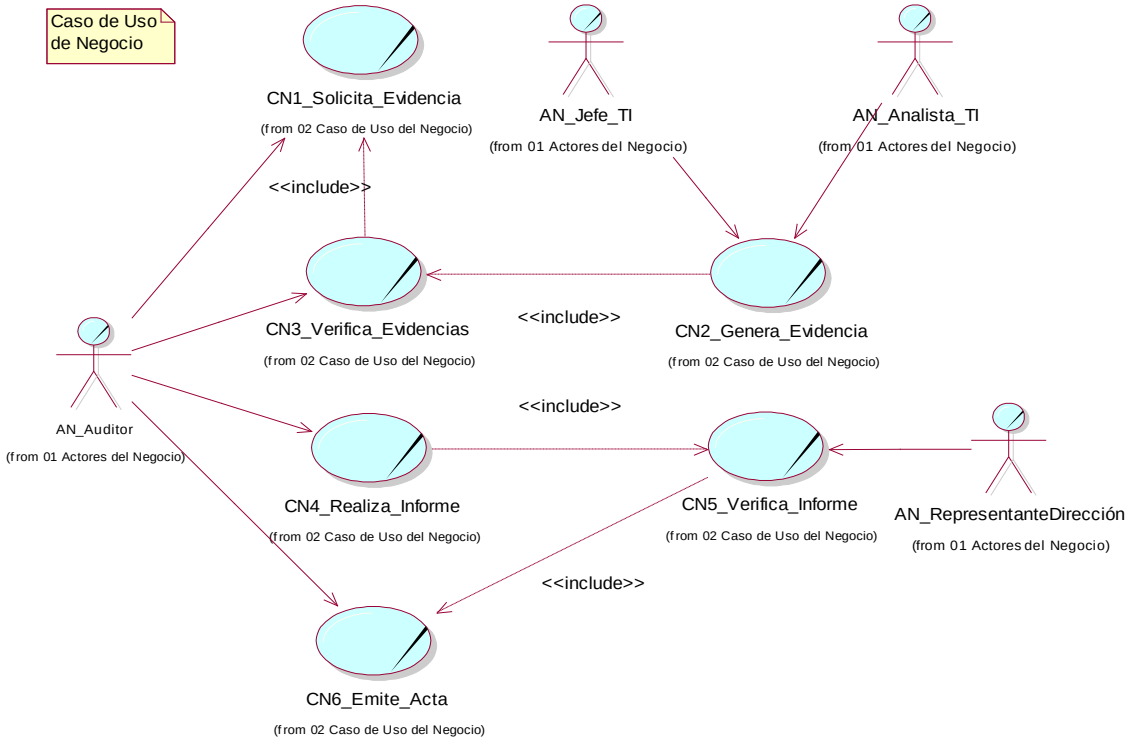


Figura N° 21 Diagrama de casos de uso del negocio
Fuente: Elaboración propia

En el diagrama se muestra la relación de los actores con sus respectivos casos de uso (Ver figura N° 21).

4.1.5. Especificación CUN más significativos

4.1.5.1. Especificación "CUN Solicitar evidencia"

Tabla 12: CUN Solicitar evidencia

Nombre	CUN_Solicitar_Evidencia
Actor del Negocio	AN_Analista_TI
Propósito	Este caso de negocio, tiene como objetivo solicitar evidencia para la validación de los controles que se tienen con referencia a seguridad de información.
Descripción	El Analista TI ingresa a cualquiera de los siguientes ítems: Contexto de la Organización - Conocimiento de la Organización y su Contexto - Partes interesadas Liderazgo - Funciones, responsabilidades y autoridad de la Organización Planificación - Acciones para enfrentar los riesgos y las oportunidades - Objetivos del SGSI Apoyo / Soporte - Competencia - Concientización - Documentación de la Información Operación - Planificación y control operacional - Evaluación de los riesgos de Seguridad de la Información - Tratamiento de los riesgos de Seguridad de la Información Sub flujos En cualquier momento el actor puede salir del sistema.
Pre-condición	El analista de TI debe de haberse identificado en el sistema.
PostCondición	Solicitud de evidencia

Fuente: Elaboración propia

En la tabla “CUN Solicitar evidencia” se especifica el flujo que realiza el analista de TI para solicitar evidencia de controles de seguridad de información (Ver tabla 12).

Tabla 13: CUN Verificar evidencia

Nombre	CUN_Verificar_Evidencia
Actor del Negocio	AN_Analista_TI
Propósito	Este caso de negocio, tiene como objetivo verificar evidencia para la validación de los controles que se tienen con referencia a seguridad de información.
Descripción	Flujo Básico 1. El Analista TI deberá ingresar a cualquiera de los siguientes ítems: Liderazgo - Política Mejora - No Conformidad y acción Correctiva - Mejora Continua 2. El Analista TI deberá presionar el botón “Subir Documento”. 3. El sistema le permitirá selección un documento y subirlo al sistema. 4. El sistema le indicará que el correo ha sido enviado con éxito. 5. El Analista TI sale del sistema. Sub flujos En cualquier momento el actor puede salir del sistema.
Pre-condición	El analista de TI debe de haber solicitado la evidencia
Flujo alternativo	Ninguno
PostCondición	Verificación de evidencia

Fuente: Elaboración propia

En la tabla “Verificar evidencia” se especifica el flujo que realiza el analista de TI para verificar evidencia (Ver tabla 13).

4.2. Requerimientos del producto / software

4.2.1. Diagrama de paquetes

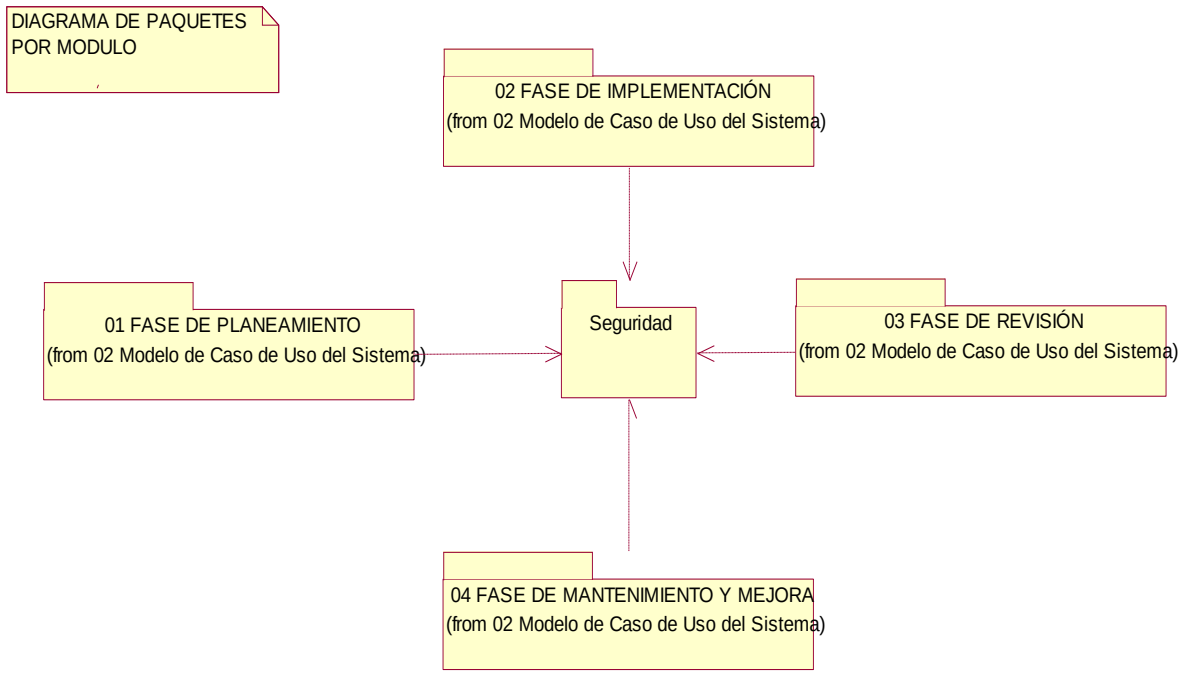


Figura N° 22 Diagrama de paquetes
Fuente: Elaboración propia

En el diagrama se muestra las fases de implementación del sistema, el cual se ha dividido en Planeamiento, implementación, revisión y mantenimiento mejora (Ver Figura N°22).

4.2.2. Interfaces con otros sistemas

No Aplica.

4.2.3. Requerimientos funcionales

- El jefe de seguridad de TI gestiona (crea, modifica, elimina, habilita/deshabilita, asigna rol) a los usuarios que utilizan el sistema.
- El administrador gestiona las restricciones (accesos) de cada tipo de rol para cada proceso.
- El analista de TI administra las plantillas (política, procedimientos, etc).

- El analista de TI planea reuniones, charlas, correos informativos, mensajes sobre la seguridad de la información.
- El analista de TI gestiona la evidencia otorgada por los jefes de área de la organización.
- El jefe de seguridad de TI revisa la documentación realizada por el analista de TI.
- El jefe de seguridad de TI administra los riesgos; los registra y clasifica el riesgo o vulnerabilidades de la organización.
- El jefe de seguridad de TI define el organigrama y las políticas.
- El representante de alta dirección aprueba la documentación definida y otorgada por el analista y jefe de seguridad de TI.
- El representante de alta dirección define la matriz RASCI y el alcance.
- El auditor interno revisa la evidencia otorgada por el jefe de TI, y emite un informe sobre los hallazgos encontrados (descripción, tipo de hallazgo).
- El representante de alta dirección revisa el informe realizado por el auditor.
- El auditor emite el acta con la aprobación del informe por parte de la alta dirección.

4.2.4. Requerimientos no funcionales

Usabilidad

- **RNF1**: El sistema debe permitir ser usado intuitivamente por cualquier usuario.
- **RNF2**: El lenguaje utilizado en la interfaz gráfica debe respetar los términos usados en el negocio y deberá ser amigable.
- **RNF3**: La interfaz gráfica deberá organizarse por secciones para una mejor comprensión.
- **RNF4**: Si el usuario genera con el ingreso de información alguna inconsistencia en el sistema, se deberá mostrar el mensaje de error adecuado y amigable.

Seguridad

- **RNF5**: El ingreso al sistema estará restringido por contraseñas cifradas y usuarios definidos.
- **RNF6**: El control de acceso implementado debe permitir asignar los perfiles para cada uno de los roles.

- **RNF7**: El sistema deberá contar con mecanismos que permitan el registro de actividades con identificación de los usuarios que los realizaron.

Confiabilidad

- **RNF8**: Las modificaciones realizadas en la base de datos se guardan en disco antes que finalicen los cambios para poder reconstruir dichas modificaciones cuando el sistema se reinicie después del fallo.
- **RNF9**: El sistema deberá manejar transacciones en las operaciones a realizar a la base de datos, en caso de falla se deberá revertir todos los procesos realizados.
- **RNF10**: El sistema deberá validar los campos, para evitar errores en el ingreso de la información.

Rendimiento

- **RNF11**: El sistema debe permitir la concurrencia de muchos usuarios a la vez.
- **RNF12**: El sistema debe tener la propiedad de escalabilidad.
- **RNF13**: El sistema tendrá continuidad.

Soporte

- **RNF14**: El sistema deberá soportar el navegador Firefox, Chrome y Opera.
- **RNF15**: Para el desarrollo de la base de datos, el sistema debe utilizar Microsoft SQL server Managment Studio.
- **RNF16**: El sistema debe estar automatizado en Bizagi Studio.

Diseño

- **RNF17**: La arquitectura tecnológica deberá considerarse en entorno web.
- **RNF18**: Se aplicara la arquitectura cliente servidor

Integraciones

- **RNF19**: No lleva ninguna integración.

4.2.5. Casos de Uso del Sistema

4.2.5.1. Diagrama de actores del Sistema

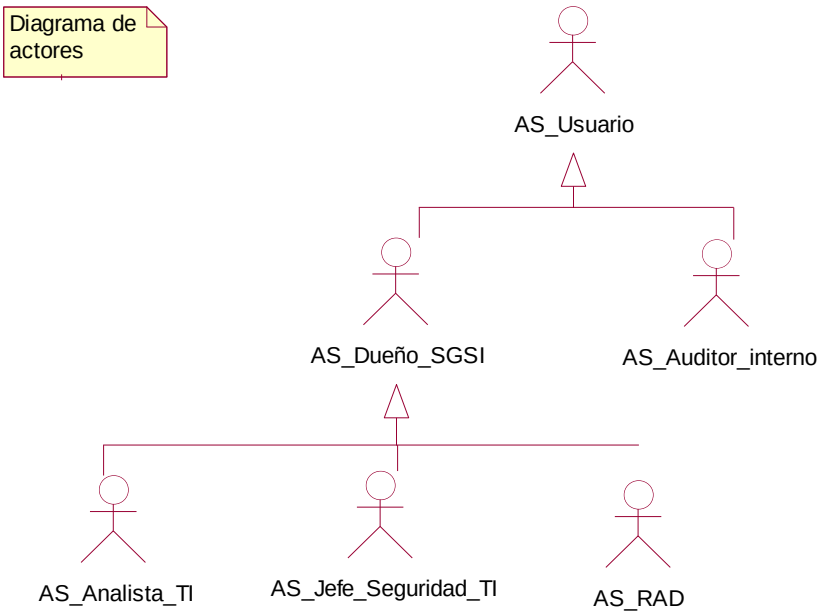


Figura N° 23 Diagrama de paquetes
Fuente: Elaboración propia

Los usuarios del sistema son el analista de TI, jefe de seguridad TI y el representante de la alta dirección (RAD), quienes son los que utilizarán el sistema (Ver figura 23).

- **As_Analista_TI**

  Este actor del sistema se encarga de administrar las plantillas, comunicar los cambios (políticas, procedimientos, cambios en la documentación).

- **AS_Jefe_Seguridad_TI**

  Este actor del sistema se encarga de revisar la documentación que realiza el analista de TI, en el caso de que el jefe de seguridad encuentre inconsistencia, entonces lo retorna al analista con sus observaciones.

- **AS_RAD**

  Este actor del sistema se encarga de aprobar la documentación.

- **AS_Auditor_Interno**

  Este actor del sistema se encarga de revisar las evidencia, y emite un acta conforme a los hallazgos (observaciones) encontrados.

4.2.5.2. Casos de uso del sistema

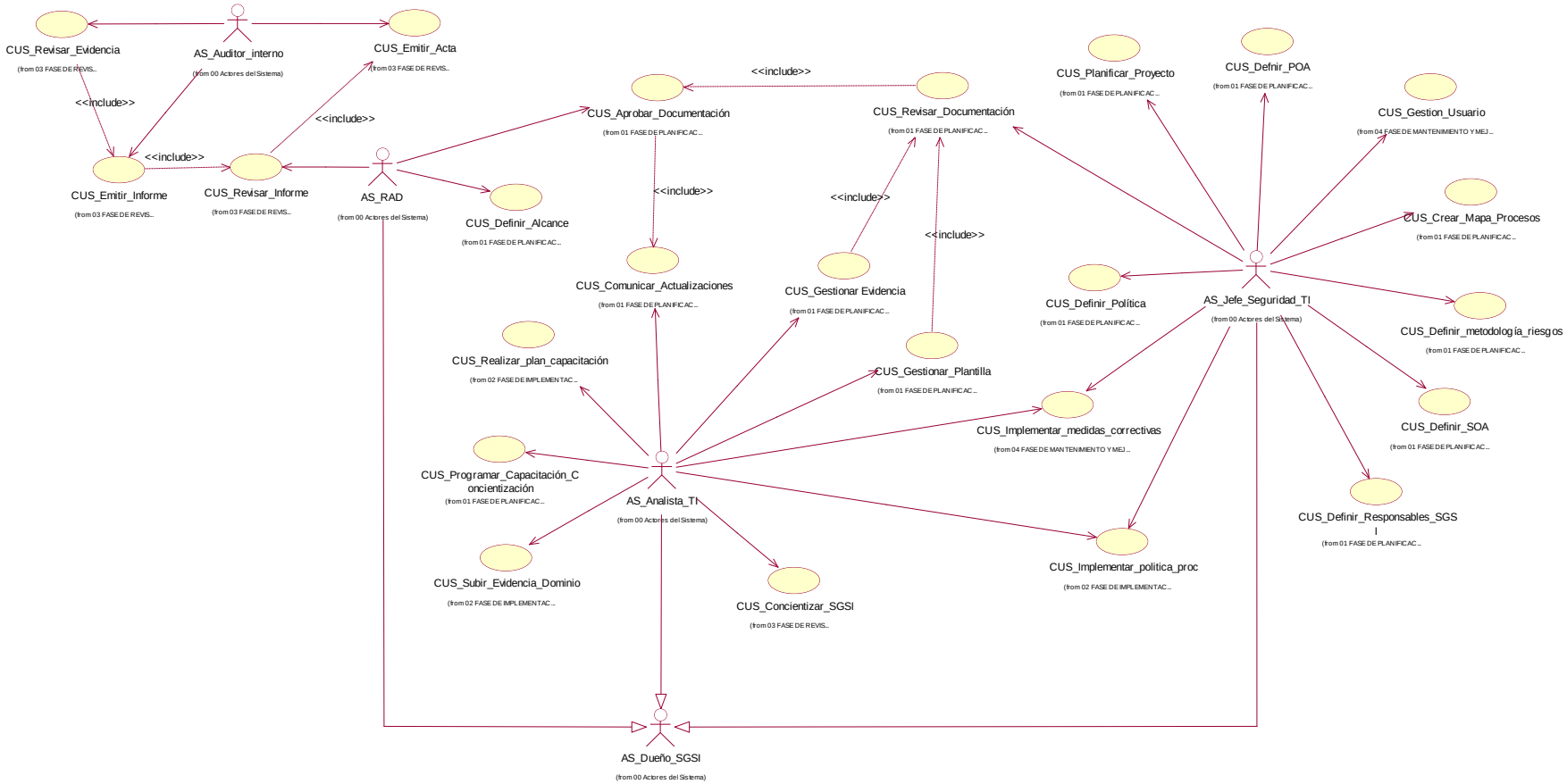


Figura N° 24 Diagrama de casos de uso del sistema
Fuente: Elaboración propia

En el diagrama se muestra las actividades que realizan los actores del sistema con los respectivos casos de uso (Ver figura N° 24)

4.2.6. Especificación CUS más significativos

4.2.6.1. Especificación Crear Mapa de procesos

Tabla 14: ECUS: CUS_Crear_Mapa_de_Procesos

Nombre	CUS_Crear_Mapa_de_Procesos
Actor del Negocio	AS_Jefe_de_seguridad_de_TI
Propósito	El caso de uso tiene como objetivo que el jefe de seguridad TI pueda crear el mapa de procesos.
Descripción	1. El jefe de seguridad TI ingresa a la opción “Crear Mapa de procesos”. 2. El sistema muestra la interfaz “Crear Mapa de procesos” que contiene la plantilla de mapa de procesos (procesos estratégicos, procesos principales/tácticos y procesos de apoyo). 3. El jefe de seguridad TI presionara en el botón “Crear Procesos” y presionara en la sección procesos principales. 4. El sistema solicitara que ingresemos el nombre del proceso. 5. El jefe de seguridad TI ingresara el nombre al proceso. 6. El jefe de seguridad TI selecciona el botón de “procedimientos” y presiona en una de las 3 secciones de procesos o dentro de un proceso. 7. El sistema solicitara el nombre del procedimiento. 8. El jefe de seguridad TI ingresara el nombre del procedimiento. 9. El jefe de seguridad usara el botón de “relación” y seleccionara los 2 objetos que quiere relacionar. 10. El jefe de seguridad TI presiona el botón “Guardar”. 11. El sistema guarda el mapa de procesos. 12. El jefe de seguridad TI sale del sistema.
Pre-condición	El jefe de seguridad de TI debe de haberse identificado en el sistema.
Flujo alternativo	Ninguno
PostCondición	Se creó el mapa de procesos con éxito.

Fuente: Elaboración propia

En la tabla “Crear mapa procesos” se especifica el flujo que realiza el jefe de seguridad TI para crear el mapa de procesos (Ver tabla 14).

4.2.6.2. Especificación Definir alcance

Tabla 15: ECUS: CUS_Definir_Alcance

Nombre	CUS_Definir_Alcance
Actor del Negocio	AS_Jefe_de_seguridad_de_TI
Propósito	El caso de uso tiene como objetivo que el jefe de seguridad TI pueda definir el alcance.
Descripción	1. El jefe de seguridad TI ingresa a la opción “Definir Alcance”. 2. El sistema muestra la interfaz “Definir Alcance”. 3. El jefe de seguridad TI Ingresa en alcance. 4. El jefe de seguridad TI presiona el botón “Guardar” 5. El sistema comprueba la información y la guarda. 6. El sistema consulta si desea generar PDF. 7. Si el jefe de seguridad TI indica que SI se procede con la generación del documento. 8. Si el jefe de seguridad TI indica que NO, se procede con la salida del sistema. 9. El sistema guarda los cambios. 10. Continúa al siguiente flujo.
Pre-condición	El jefe de seguridad de TI debe de haberse identificado en el sistema.
Flujo alternativo	Ninguno
PostCondición	Se definió el alcance con éxito.

Fuente: Elaboración propia

En la tabla “Definir Alcance” se especifica el flujo que realiza el jefe de seguridad TI para definir el alcance que se tendrá en el sistema de gestión de seguridad de la información (Ver tabla 15).

Tabla 16: ECUS: CUS_Definir_Organigrama_SGSI

Nombre	CUS_Definir_Organigrama_SGSI
Actor del Negocio	AS_Jefe_de_seguridad_de_TI
Propósito	El caso de uso tiene como objetivo definir un organigrama para el sistema.
Descripción	1.El Jefe de Seguridad TI ingresa al ítem "Apoyo/Soporte", ahí seleccionará la opción "Recursos". 2.El sistema le dará la opción de ingresar los nombres de los responsables de cada dominio. 3.El Jefe de Seguridad TI almacenará la información presionando el botón "Guardar". 4.El Jefe de Seguridad TI sale del sistema.
Pre-condición	El jefe de seguridad de TI debe de haberse identificado en el sistema.
PostCondición	Se registró el organigrama con éxito.

Fuente: Elaboración propia

En la tabla "Definir organigrama SGSI" se especifica el flujo que realiza el jefe de seguridad TI para definir el organigrama realizado para el SGSI (Ver tabla 16).

Tabla 17: ECUS: CUS_Definir_Matriz_RASCI

Nombre	CUS_Definir_Matriz_RASCI
Actor del Negocio	AS_Jefe_de_seguridad_de_TI
Propósito	El objetivo es definir responsables según cada dominio de SGSI.
Descripción	1. El Jefe de Seguridad TI deberá ingresar al ítem "Liderazgo" y seleccionar la opción "Funciones, responsabilidades y autoridades de la organización". 2. El sistema le permitirá ingresar los cargos de acuerdo a la empresa. 3. Después de ingresado los cargos, se deberá establecer las funciones. 4. El Jefe de Seguridad TI almacenará la información presionando el botón "Guardar". 5. El Jefe de Seguridad TI sale del sistema.
Pre-condición	El jefe de seguridad de TI debe de haberse identificado en el sistema.
PostCondición	Se define la matriz RASCI con éxito.

Fuente: Elaboración propia

En la tabla “Definir matriz RASCI” se especifica el flujo que realiza el jefe de seguridad TI para definir cada uno de los roles y responsabilidades dentro del sistema de gestión de seguridad de la información (Ver tabla 17).

Tabla 18: ECUS: CUS_Definir_SOA

Nombre	CUS_Definir_SOA
Actor del Negocio	AS_Jefe_de_seguridad_de_TI
Propósito	El caso de uso tiene como objetivo que el jefe de seguridad TI pueda definir la matriz SOA.
Descripción	1. El jefe de seguridad TI ingresa a la opción “Definir SOA”. 2. El sistema muestra la interfaz “Definir SOA” que contiene a la matriz SOA. 3. El jefe de seguridad TI llena en cada punto de la matriz SOA los siguientes campos: Aplica? (si o no), justificación, Estado Actual, Nivel de madurez del control y clasificación (muy baja, baja alta o muy alta) 4. El jefe de seguridad TI presiona el botón “Guardar”. 5. El sistema valida los datos ingresados y guarda la matriz SOA. 6. El sistema guarda los cambios efectuados por parte del jefe de seguridad TI.
Pre-condición	El jefe de seguridad de TI debe de haberse identificado en el sistema.
Flujo alternativo	Ninguno
PostCondición	Se definió la matriz SOA con éxito.

Fuente: Elaboración propia

En la tabla “Definir SOA” se especifica el flujo que realiza el jefe de seguridad TI para definir la matriz de aplicabilidad de los dominios según el alcance definido por el responsable de la alta dirección (Ver tabla 18).

Tabla 19: ECUS: CUS_Solicitar_Plantilla

Nombre	CUS_Solicitar_Plantilla
Actor del Negocio	AS_Jefe_de_seguridad_de_TI, As_Analista_TI
Propósito	Solicitar el llenado de las plantillas para posteriormente subirlos como evidencia del control.
Descripción	1. El Analista TI ingresa a cualquiera de los siguientes ítems: *Contexto de la Organización* - Conocimiento de la Organización y su Contexto - Partes interesadas *Liderazgo* - Funciones, responsabilidades y autoridad de la Organización Planificación - Acciones para enfrentar los riesgos y las oportunidades - Objetivos del SGSI *Apoyo / Soporte* - Competencia - Concientización - Documentación de la Información *Operación* - Planificación y control operacional - Evaluación de los riesgos de Seguridad de la Información - Tratamiento de los riesgos de Seguridad de la Información *Evaluación del Desempeño* - Monitoreo, medición, análisis y evaluación - Auditorías internas - Revisión por parte de la Dirección 2. El Analista TI ingresa a la opción “Solicitar Plantilla”. 3. Él ingresa la información requerida por la plantilla. 4. Sube el archivo al sistema. 5. El sistema le indicará que la plantilla ha sido ingresada con éxito. 6. El Analista TI sale del sistema.
Pre-condición	El Analista TI debe haberse identificado en el sistema.
Flujo alternativo	Ninguno
PostCondición	Se subió plantilla con éxito.

Fuente: Elaboración propia

En la tabla “Solicitar plantillas” se especifica el flujo que realiza el jefe de seguridad TI para el llenado de las plantillas de acuerdo a cada uno de los controles según la norma (Ver tabla 19).

4.3. Análisis y Diseño

4.3.1. Análisis

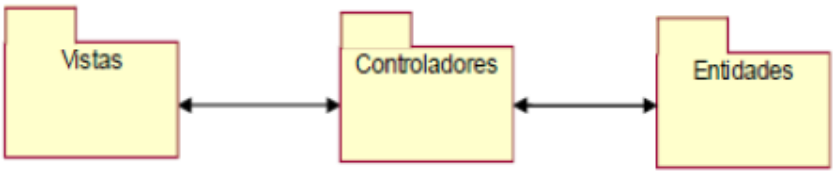


Figura N° 25 Diagrama de clases de análisis
Fuente: Elaboración propia

En el diagrama se muestra la relación de los paquetes de clases que se utilizan para la estructura del sistema (Ver Figura N°25).

4.3.2. Diseño

Solicitar Plantilla

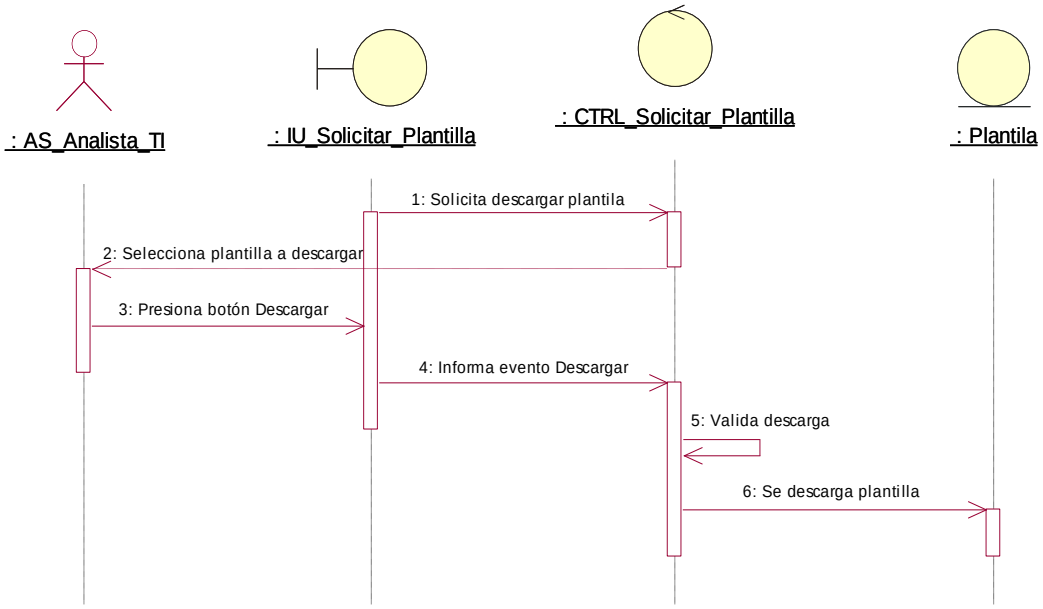


Figura N° 26 Diagrama de secuencia Solicitar Plantilla
Fuente: Elaboración propia

Se muestra en el diagrama de secuencia el caso de uso “Solicitar plantilla” que está a cargo del analista de TI (Ver figura N° 26).

Subir Documento

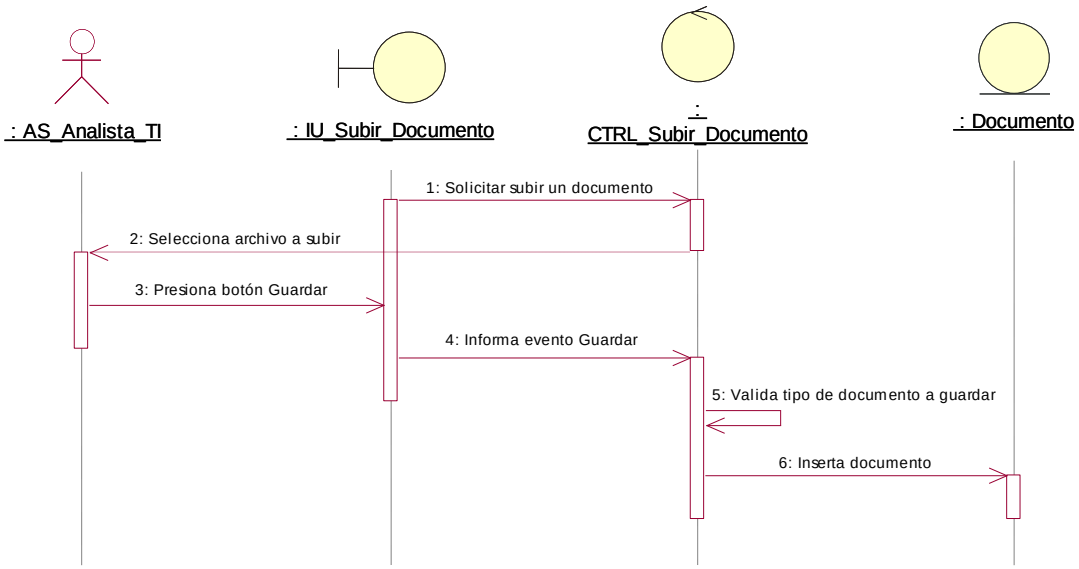


Figura N° 27 Diagrama de secuencia Solicitar Plantilla
Fuente: Elaboración propia

Se muestra en el diagrama de secuencia el caso de uso “Subir documento” que está a cargo del analista de TI (Ver figura 27).

4.3.3. Modelo de Datos

4.3.3.1. Modelo lógico; en el cual se describen aspectos relacionados con la organización, y se recopilan datos y la relación que existe entre ellos (Ver Figura N° 28).

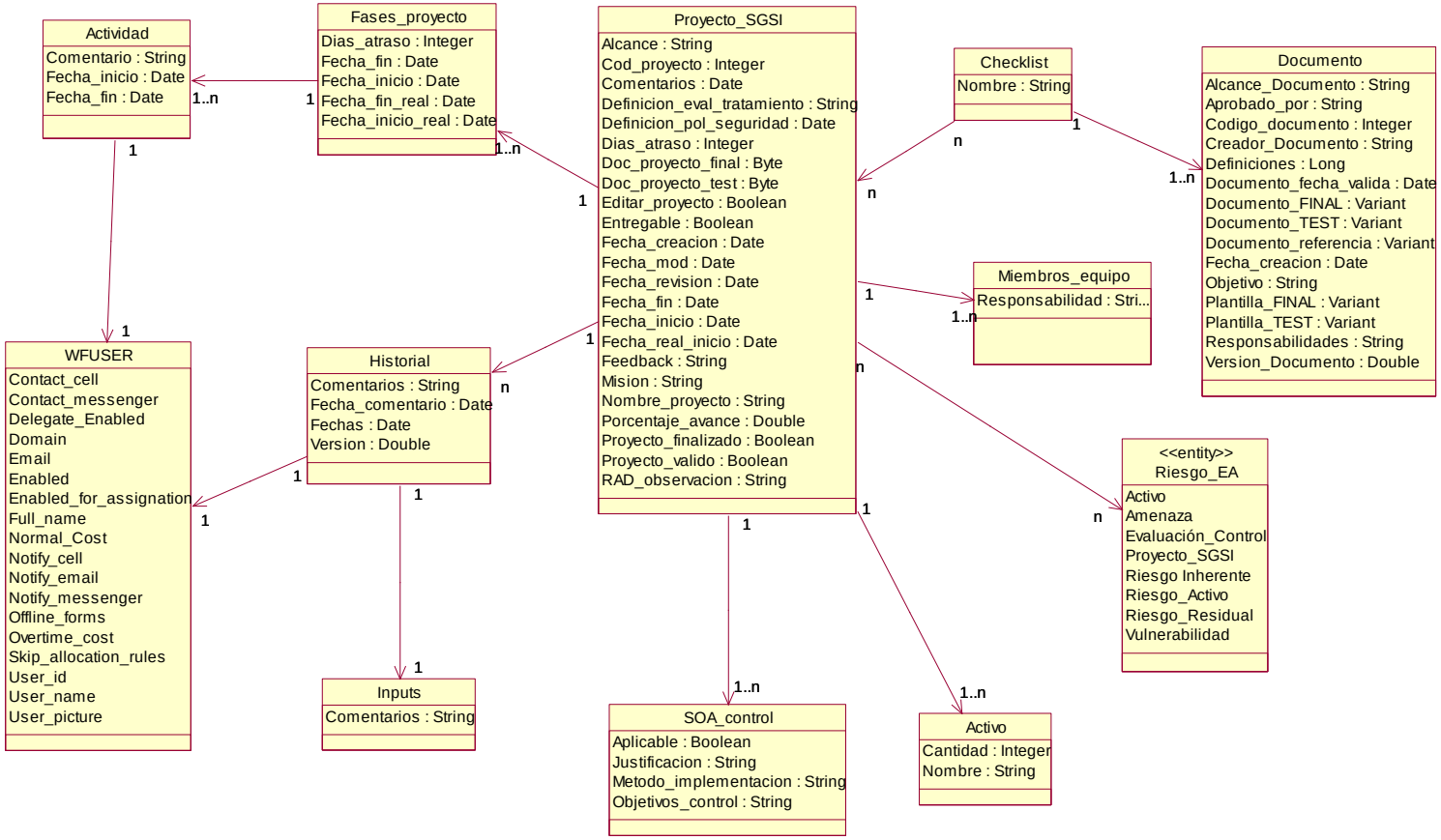


Figura N° 28: Modelo lógico
Fuente: Elaboración propia

4.3.3.2. Modelo físico, es la relación que existe entre los datos obtenido de la compañía (Ver Figura N° 29).

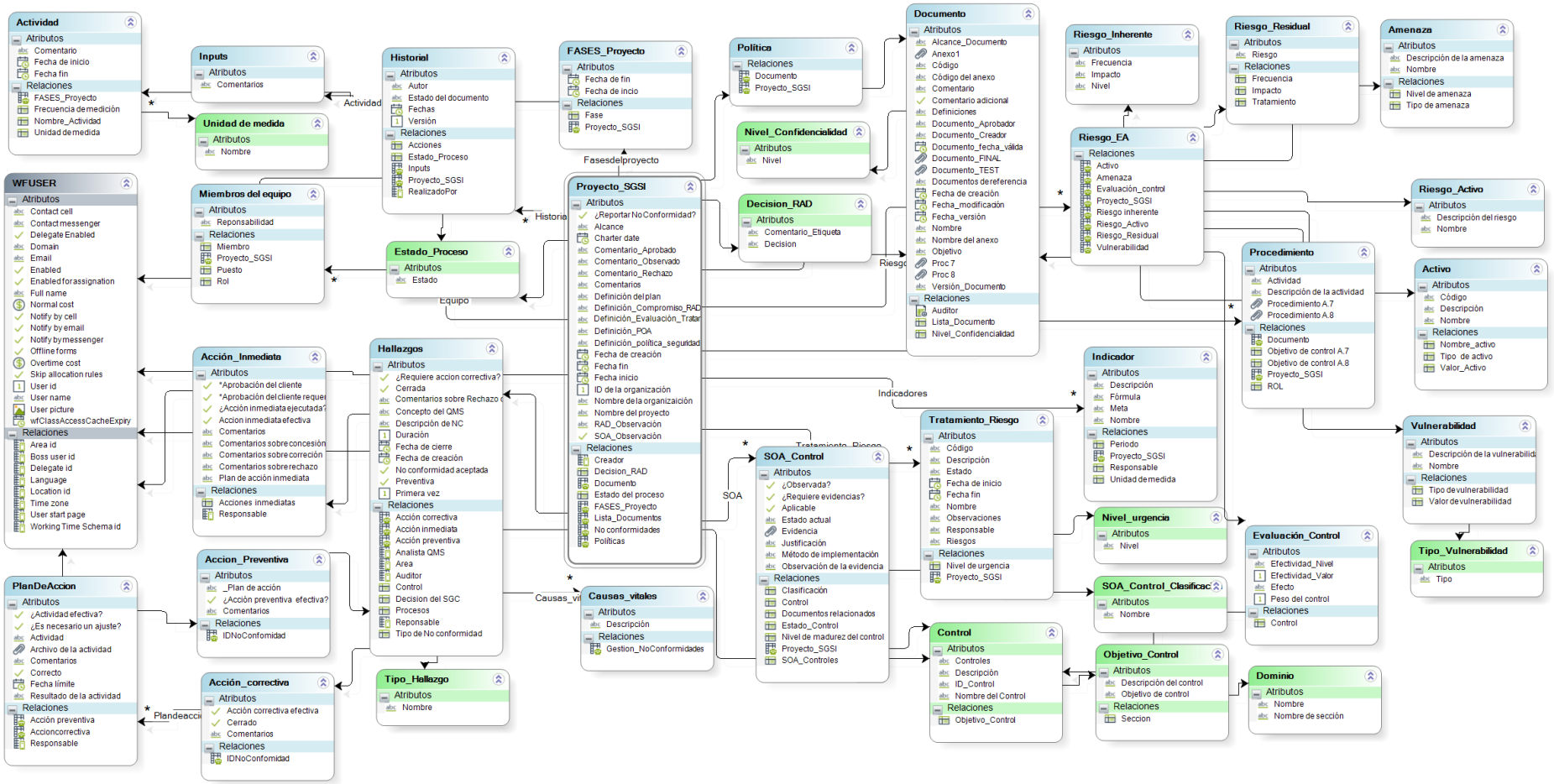


Figura N° 29: Modelo físico
Fuente: Elaboración propia

4.3.3.3. Diccionario de Datos

Es un listado organizado con la descripción de los datos que utilizamos en el sistema. (Ver tabla 20- 56).

Tabla 20: Estructura de la tabla maestra Proyecto_SGSI

Nombre	Proyecto_SGSI
Descripción	Representa la información de los proyectos.
Atributo	**Tipo de dato**
ID_PROYECTO	ENTERO
ALCANCE	TEXTO (200)
CODIGO_PROYECTO	TEXTO (50)
COMENTARIOS	TEXTO (500)
ENTREGABLE	TEXTO (300)
MISION	TEXTO (300)
NOMBREDELPROYECTO	TEXTO (100)
RAD_OBSERVACION	TEXTO (1000)
DEFINICIONPOLITICASEGURIDA	TEXTO (1000)
RIESGOEVALUATRATAM	TEXTO (1000)
FECHADECREACION	FECHA - HORA
FECHADEMODIFICACION	FECHA - HORA
FECHADEREVISION	FECHA – HORA
FECHAFIN	FECHA – HORA
FECHAINICIO	FECHA – HORA
FECHAREALDEINICIO	FECHA – HORA
PORCENTAJEDEAVANCE	FLOTANTE
EDITARPROYECTO	BOOLEANO (SI – NO)
DIASDEATRASO	ENTERO
ID_CREADOR	ENTERO
ID_DECISION_RAD	ENTERO
ID_ESTADODELPROCESO	ENTERO
ID_DOCUMENTO	ENTERO
ID_CHECKLIST	ENTERO
ID_CHECKLIST	ENTERO
ID_SOA	ENTERO
ID_ACTIVO	ENTERO
ID_EQUIPO	ENTERO
ID_HISTORIAL	ENTERO

Fuente: Elaboración propia

Tabla 21: Estructura de la tabla maestra FASES_Proyecto

Nombre	FASES_Proyecto
Descripción	Representa la información respecto a la planificación de las fases en un proyecto.
Atributo	**Tipo de dato**
ID_FASESPROYECTO	ENTERO
FECHADEINCIO	FECHA - HORA
FECHADEFIN	FECHA - HORA
ID_PROYECTO_SGSI	ENTERO

Fuente: Elaboración propia

Tabla 22: Estructura de la tabla maestra Actividad

Nombre	Actividad
Descripción	Representa la información de las actividades de cada fase.
Atributo	**Tipo de dato**
ID_ActividaD	ENTERO
COMENTARIO	TEXTO (400)
FECHADEINICIO	FECHA - HORA
FEHAFIN	FECHA - HORA
ID_NOMBREACTIVIDAD	ENTERO
ID_FASES_PROYECTO	ENTERO
ID_FRECUENCIADEMEDICION	ENTERO
ID_UNIDADDEMEDIDA	ENTERO
ID_RESPONSABLE	ENTERO

Fuente: Elaboración propia

Tabla 23: Estructura de la tabla maestra Checklist

Nombre	Checklist
Descripción	Representa la información del checklist.
Atributo	**Tipo de dato**
ID_CHECKLIST	ENTERO
NOMBRE	TEXTO (100)
ID_PROYECTO_SGSI	ENTERO

Fuente: Elaboración propia

Tabla 24: Estructura de la tabla paramétrica FASE

Nombre	FASE
Descripción	Representa las fases del proyecto.
Atributo	**Tipo de dato**
ID_FASE	ENTERO
NOMBRE	TEXTO (50)

Fuente: Elaboración propia

Tabla 25: Estructura de la tabla paramétrica FASE

Nombre	DECISION_RAD
Descripción	Representa la decisión del RAD
Atributo	**Tipo de dato**
ID_FASE	ENTERO
COMENTARIO_ETIQUETA	TEXTO (80)
DECISION	TEXTO (200)

Fuente: Elaboración propia

Tablas del Historial

Tabla 26: Estructura de la tabla maestra Historial

Nombre	Historial
Descripción	Representa el historial de las acciones de cada proceso.
Atributo	**Tipo de dato**
ID_HISTORIAL	ENTERO
COMENTARIOS	TEXTO (200)
FECHAS	FECHA - HORA
FECHA DEL COMENTARIO	FECHA - HORA
VERSIÓN	ENTERO
ID_ACCIONES	ENTERO
ID_ESTADO_PROCESO	ENTERO
ID_INPUTS	ENTERO
ID_PROYECTO_SGSI	ENTERO
ID_REALIZADOPOR	ENTERO

Fuente: Elaboración propia

Tabla 27: Estructura de la tabla maestra Inputs

Nombre	Inputs
Descripción	Representa la información de los comentarios del historial.
Atributo	**Tipo de dato**
ID_Inputs	ENTERO
Comentario	TEXTO (200)

Fuente: Elaboración propia

Tabla 28: Estructura de la tabla paramétrica Estado_Proceso

Nombre	Estado_Proceso
Descripción	Representa la información de los estados del proceso.
Atributo	**Tipo de dato**
ID_Estado_Proceso	ENTERO
Estado	TEXTO (50)

Fuente: Elaboración propia

Tabla 29: Estructura de la tabla paramétrica Acciones

Nombre	Acciones
Descripción	Representa la información de las acciones del proceso.
Atributo	**Tipo de dato**
ID_ACCION	ENTERO
ACCION	TEXTO (80)

Fuente: Elaboración propia

Tablas de los Miembros de equipo

Tabla 30: Estructura de la tabla maestra Miembros del equipo

Nombre	Miembros_equipo
Descripción	Representa la información de las responsabilidades de los miembros del equipo.
Atributo	**Tipo de dato**
ID_MIEMBROS_EQUIPO	ENTERO
RESPONSABILIDAD	TEXTO (1000)
ID_MIEMBRO	ENTERO
ID_PROYECTO_SGSI	ENTERO
ID_AREA_ROL	ENTERO

Fuente: Elaboración propia

Tabla 31: Estructura de la tabla paramétrica Miembro

Nombre	Miembro
Descripción	Representa la información de cada miembro del equipo
Atributo	**Tipo de dato**
ID_MIEMBRO	ENTERO
NOMBRE	TEXTO (100)
ID_USERROLE	ENTERO

Fuente: Elaboración propia

Tablas de los Documentos

Tabla 32: Estructura de la tabla maestra Documento

Nombre	Documento
Descripción	Representa la información del contenido de los documentos.
Atributo	**Tipo de dato**
ID_DOCUMENTO	ENTERO
ALCANCE_DOCUMENTO	TEXTO (1000)
APROBADO POR	TEXTO (50)
CÓDIGO_DOCUMENTO	ENTERO
CREADOR_DOCUMENTO	ENTERO
DEFINICIONES	TEXTO (800)
DOCUMENTO_FINAL	ARCHIVO
DOCUMENTO_TEST	ARCHIVO
DOCUMENTO_FECHA_VÁLIDA	FECHA - HORA
DOCUMENTOS_REFERENCIA	TEXTO (800)
FEHADECREACION	FECHA - HORA
OBJETIVO	TEXTO (800)
PLANTILLA_FINAL	ARCHIVO
PLANTILLA_TEST	ARCHIVO
RESPONSABILDIADES	TEXTO (800)
VERSION_DOCUMENTO	TEXTO (800)
ID_DECISION_RAD	ENTERO
ID_TIPO_DOCUMENTO	ENTERO
ID_NOMBRE_PLANTILLA	ENTERO
ID_NOMBRE_DOCUMENTO	ENTERO
ID_NIVELDECONFIDENCIALIDAD	ENTERO
ID_ESTADO_DOCUMENTO	ENTERO
ID_CHECKLIST	ENTERO

Fuente: Elaboración propia

Tabla 33: Estructura de la tabla paramétrica Nivel de confidencialidad

Nombre	Nivel de confidencialidad
Descripción	Representa la información registrada de los niveles de confidencialidad de los documentos.
Atributo	**Tipo de dato**
ID_NOMBRE_DOCUMENTO	ENTERO
NIVEL	TEXTO (50)

Fuente: Elaboración propia

Tabla 34: Estructura de la tabla paramétrica Nombre de plantilla

Nombre	Nombre_Plantilla
Descripción	Representa la información registrada de los nombres de las plantillas.
Atributo	**Tipo de dato**
ID_NOMBRE_PLANTILLA	ENTERO
CODIGO_PLANTILLA	TEXTO (50)
DESCRIPCION	TEXTO (800)
NOMBRE	TEXTO (100)
PLANTILLA_ARCHIVO	ARCHIVO

Fuente: Elaboración propia

Tabla 35: Estructura de la tabla paramétrica Tipo de documento

Nombre	Tipo_Documento
Descripción	Representa la información registrada de los tipos de documentos.
Atributo	**Tipo de dato**
ID_TIPO_DOCUMENTO	ENTERO
TIPO	TEXTO (50)

Fuente: Elaboración propia

Tabla 36: Estructura de la tabla paramétrica Nombre_Documento

Nombre	Nombre_Documento
Descripción	Representa la información de los nombres de los documentos
Atributo	**Tipo de dato**
ID_NOMBRE_DOCUMENTO	ENTERO
NOMBRE	TEXTO (200)

Fuente: Elaboración propia

Tablas de los controles de la ISO 27001

Tabla 37: Estructura de la tabla maestra SOA_Control

Nombre	SOA_CONTROL
Descripción	Representa la información de la declaración de aplicabilidad (SOA).
Atributo	**Tipo de dato**
ID_SOA_CONTROL	ENTERO
APLICABLE	BOOLEANO (SI – NO)
JUSTIFICACIÓN	TEXTO (800)
MÉTODODEIMPLEMENTACIÓN	TEXTO (300)
OBJETIVOS DE CONTROL	TEXTO (300)
ID_CONTROL	ENTERO
ID_ESTADO_CONTROL	ENTERO
ID_PROYECTO_SGSI	ENTERO

Fuente: Elaboración propia

Tabla 38: Estructura de la tabla paramétrica Control

Nombre	Control
Descripción	Representa la información de los controles de la ISO 27001.
Atributo	**Tipo de dato**
ID_CONTROL	ENTERO
NOMBRE DEL CONTROL	TEXTO (200)
DESCRIPCIÓN	TEXTO (500)
PREGUNTA	TEXTO (300)
ID_OBJETIVO_CONTROL	ENTERO

Fuente: Elaboración propia

Tabla 39: Estructura de la tabla paramétrica Objetivo Control

Nombre	Objetivo_Control
Descripción	Representa la información de los objetivos de control de la ISO 27001.
Atributo	**Tipo de dato**
ID_OBJETIVO_CONTROL	ENTERO
NOMBRE_OBJETIVO_CONTROL	TEXTO (100)
DESCRIPCIÓN_OBJETIVO	TEXTO (500)
ID_DOMINIO	ENTERO

Fuente: Elaboración propia

Tabla 40: Estructura de la tabla paramétrica Dominio

Nombre	Dominio
Descripción	Representa la información de los dominios la ISO 27001.
Atributo	**Tipo de dato**
ID_DOMINIO	ENTERO
NOMBRE_DOMINIO	TEXTO (100)

Fuente: Elaboración propia

Tabla 41: Estructura de la tabla paramétrica Estado

Nombre	Estado
Descripción	Representa la información de los estados de la matriz de aplicabilidad.
Atributo	**Tipo de dato**
ID_ESTADO	ENTERO
NOMBRE_ESTADO	TEXTO (100)

Fuente: Elaboración propia

Tablas del Hallazgo

Tabla 42: Estructura de la tabla maestra hallazgos

Nombre	Hallazgo
Descripción	Representa la información de las observaciones encontradas en la auditoría.
Atributo	**Tipo de dato**
ID_HALLAZGO	ENTERO
DESCRIPCION	TEXTO (500)
DURACION	FLOTANTE
FECHA_CREACION	FECHA - HORA
FECHA_CIERRE	FECHA - HORA
PREVENTIVA	BOOLEANO (SI – NO)
REQUIERE_ACCION_CORRECTIVA	BOOLEANO (SI – NO)
ID_TIPO_HALLAZGO	ENTERO
ID_CONTROL	ENTERO
ID_ACCION_CORRECTIVA	ENTERO
ID_ACCION_PREVENTIVA	ENTERO
ID_CAUSDAS	ENTERO

Fuente: Elaboración propia

Tabla 43: Estructura de la tabla maestra Plan de acción

Nombre	PlanDeAccion	
Descripción	Representa la información del plan de acción.	
Atributo		**Tipo de dato**
ID_PLANDEACCION		ENTERO
ARCHIVO_ACTIVIDAD		ARCHIVO
COMENTARIO		TEXTO (300)
FECHA_LIMITE		FECHA - HORA
CORRECTO		BOOLEANO (SI – NO)
ACTIVIDAD_EFECTIVA		BOOLEANO (SI – NO)
NECESARIO_CAMBIOS		BOOLEANO (SI – NO)
ID_ACCION_CORRECTIVA		ENTERO
ID_ACCION_PREVENTIVA		ENTERO

Fuente: Elaboración propia

Tabla 44: Estructura de la tabla maestra Acción Preventiva

Nombre	Acción_preventiva	
Descripción	Representa la información de la acción preventiva.	
Atributo		**Tipo de dato**
ID_ACCION_PREVENTIVA		ENTERO
COMENTARIOS		TEXTO (300)
ACCION_PREVENTIVA_EFECTIVA		BOOLEANO (SI – NO)
ID_HALLAZGO		ENTERO

Fuente: Elaboración propia

Tabla 45: Estructura de la tabla maestra Acción Correctiva

Nombre	Acción_correctiva	
Descripción	Representa la información de la acción correctiva.	
Atributo		**Tipo de dato**
ID_ACCION_CORRECTIVA		ENTERO
COMENTARIOS		TEXTO (300)
ACCION_CORRECTIVA_EFECTIVA		BOOLEANO (SI – NO)
ID_HALLAZGO		ENTERO

Fuente: Elaboración propia

Tabla 46: Estructura de la tabla maestra Causas vitales

Nombre	Causas_vitales
Descripción	Representa la información de las causas vitales de los hallazgos.
Atributo	**Tipo de dato**
ID_CAUSAS_VITALES	ENTERO
NOMBRE	TEXTO (300)
ID_HALLAZGO	ENTERO

Fuente: Elaboración propia

Tabla 47: Estructura de la tabla paramétrica Tipo de hallazgo

Nombre	Tipo_Hallazgo
Descripción	Representa la información de los tipos de hallazgos.
Atributo	**Tipo de dato**
ID_TIPO_HALLAZGO	ENTERO
NOMBRE	TEXTO (120)

Fuente: Elaboración propia

Tablas de los Riegos

Tabla 48: Estructura de la tabla maestra Riesgo

Nombre	Riesgo_EA
Descripción	Representa la información de los riesgos
Atributo	**Tipo de dato**
ID_RIESGO_EA	ENTERO
ID_ACTIVO	ENTERO
ID_AMENAZA	ENTERO
ID_EVALUACION_CONTROL	ENTERO
ID_PROYECTO_SGSI	ENTERO
ID_RIESGO_INHERENTE	ENTERO
ID_RIESGO_ACTIVO	ENTERO
ID_RIESGO_RESIDUAL	ENTERO
ID_VULNERAVILIDAD	ENTERO

Fuente: Elaboración propia

Tabla 49: Estructura de la tabla maestra Riesgo

Nombre	Riesgo_Inherente
Descripción	Representa la información del riesgo inherente.
Atributo	**Tipo de dato**
ID_RIESGO_INHERENTE	ENTERO
FRECUENCIA	TEXTO (120)
IMPACTO	TEXTO (120)
NIVEL	TEXTO (120)

Fuente: Elaboración propia

Tabla 50: Estructura de la tabla maestra Riesgo

Nombre	Riesgo_Residual
Descripción	Representa la información del riesgo residual.
Atributo	**Tipo de dato**
ID_RIESGO_RESIDUAL	ENTERO
RIESGO	TEXTO (150)
ID_VALOR_FRECUENCIA	ENTERO
ID_VALOR_IMPACTO	ENTERO
ID_RESPUESTA_RIESGO	ENTERO

Fuente: Elaboración propia

Tabla 51: Estructura de la tabla maestra Amenaza

Nombre	Amenaza
Descripción	Representa la información de la amenaza.
Atributo	**Tipo de dato**
ID_AMENAZA	ENTERO
NOMBRE	TEXTO (100)
DESCRIPCION_AMENAZA	TEXTO (500)
ID_TIPO_AMENAZA	ENTERO
ID_VALOR_AMENAZA	ENTERO

Fuente: Elaboración propia

Tabla 52: Estructura de la tabla maestra Riesgo del activo

Nombre	Riesgo_Activo
Descripción	Representa la información de los riesgos del activo.
Atributo	**Tipo de dato**
ID_RIESGO_ACTIVO	ENTERO
NOMBRE	TEXTO (100)
DESCRIPCION_RIESGO	TEXTO (500)

Fuente: Elaboración propia

Tabla 53: Estructura de la tabla maestra Activo

Nombre	Activo
Descripción	Representa la información de los activos
Atributo	**Tipo de dato**
ID_ACTIVO	ENTERO
CODIGO_ACTIVO	TEXTO (100)
DESCRIPCION	TEXTO (500)
NOMBRE	TEXTO (100)
ID_NOMBRE_ACTIVO	ENTERO
ID_TIPO_ACTIVO	ENTERO
ID_VALOR_ACTIVO	ENTERO

Fuente: Elaboración propia

Tabla 54: Estructura de la tabla maestra vulnerabilidad

Nombre	Vulnerabilidad
Descripción	Representa la información de la vulnerabilidad de los riesgos.
Atributo	**Tipo de dato**
ID_VULNERABILIDAD	ENTERO
DESCRIPCION	TEXTO (500)
NOMBRE	TEXTO (100)
ID_TIPO_VULNERABILIDAD	ENTERO
ID_VALOR_VULNERABILIDAD	ENTERO

Fuente: Elaboración propia

Tabla 55: Estructura de la tabla maestra de evaluación del control

Nombre	Evaluación_Control
Descripción	Representa la información de la evaluación del control.
Atributo	**Tipo de dato**
ID_EVALUACION_CONTROL	ENTERO
EFECTO	TEXTO (200)
PESO_CONTROL	ENTERO
EFECTIVIDAD_VALOR	ENTERO
EFECTIVIDAD_NIVEL	TEXTO (120)
ID_CONTROL	ENTERO

Fuente: Elaboración propia

Tabla 56: Estructura de la tabla maestra del tratamiento de riesgo

Nombre	Tratamiento_Riesgo
Descripción	Representa la información de la evaluación del control.
Atributo	**Tipo de dato**
ID_TRATAMIENTO_RIESGO	ENTERO
CODIGO_TRATAMIENTO	TEXTO (10)
DESCRIPCION	TEXTO (300)
ESTADO	TEXTO (100)
FECHA_INICIO	FECHA - HORA
FECHA_FIN	FECHA - HORA
NOMBRE	TEXTO (100)
OBSERVACIONES	TEXTO (300)
RESPONSABLE	TEXTO (100)
RIESGOS	TEXTO (300)
ID_NIVEL_URGENCIA	ENTERO
ID_PROYECTO_SGSI	ENTERO

Fuente: Elaboración propia

4.4. Arquitectura del producto / software

4.4.1. Representación de la arquitectura

Ambiente de producción
La configuración del ambiente de producción en Bizagi soporta clústeres.
En este ambiente se utiliza Automation Server, y la solución se despliega considerando las siguientes capas (Ver Figura N° 30).

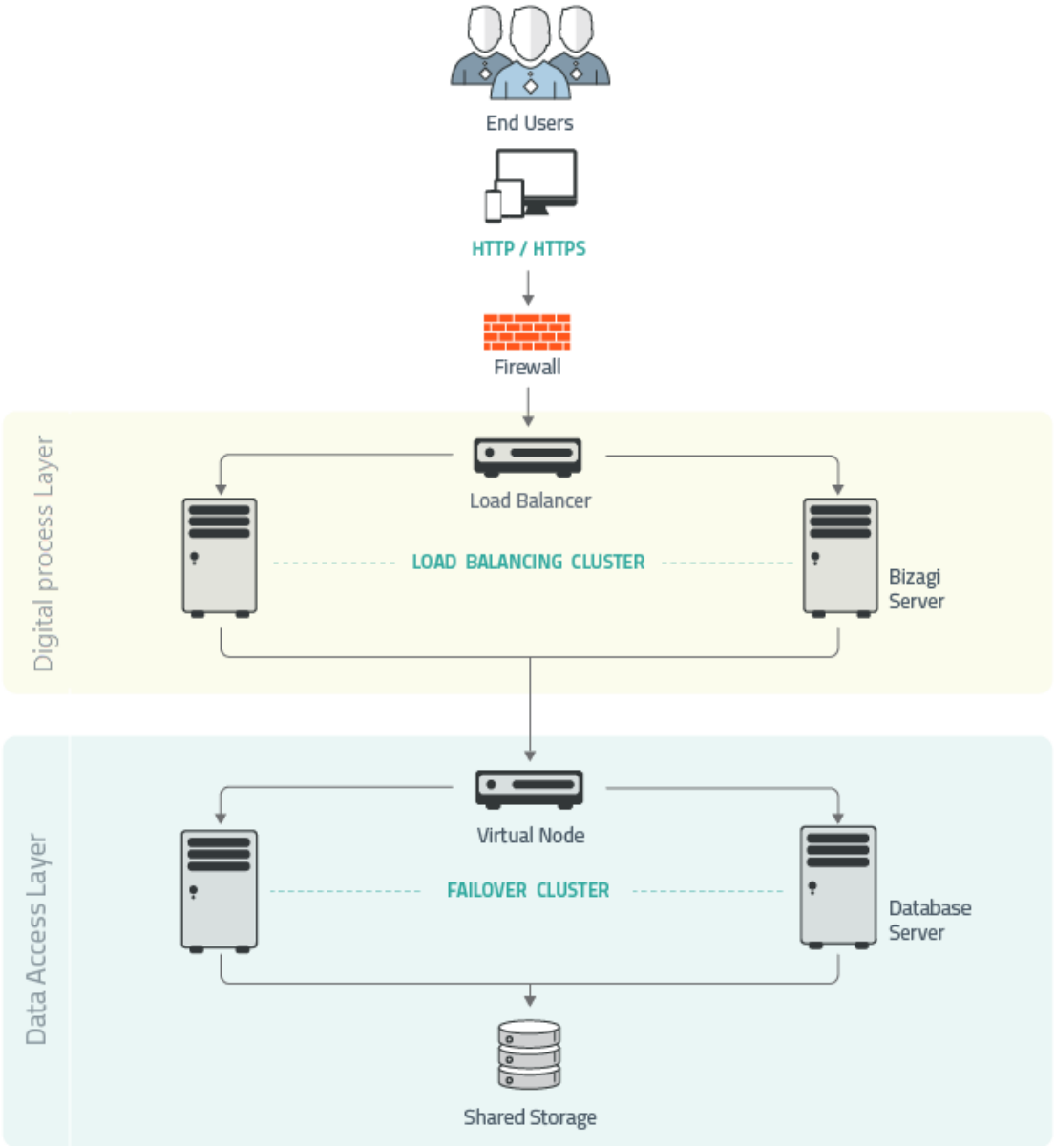


Figura N° 30 Ambiente de producción en Bizagi
Fuente: http://help.bizagi.com/bpm-suite/es/index.html?suite_producta.htm

Capa de Acceso a datos (Data Access Layer)
La Capa de Acceso a datos contiene el Servidor de base de datos y puede configurarse con un nodo para mecanismo de tolerancia a fallos.
Los motores de base de datos soportados para el modelo de Bizagi son: Microsoft SQL Server y Oracle.

Capa Bizagi (Bizagi Layer)
La Capa Bizagi contiene el Servidor Bizagi y puede configurarse como clúster con un número adicional de nodos (para el balanceo de cargas).
Bizagi soporta la ejecución de los procesos en plataformas .NET.
Cuando sus procesos se ejecutan sobre una plataforma en .NET, se usa un entorno Windows con Internet Information Services (IIS) como Servidor Web.

Opción adicional

Un servidor adicional (configuración opcional) puede ser configurado para publicar los procesos de Bizagi en Internet.

En esta configuración, el Servidor Bizagi se mantiene en la intranet y un proxy será utilizado en la DMZ para redirigir el acceso desde Internet, de manera segura.

4.4.2. Vista de Casos de Uso

4.4.2.1. Diagramas de casos de uso más significativos, en el cual se describe los casos más representativos utilizados, además los que se realizaron para la priorización del alcance (Ver Figura N° 31).

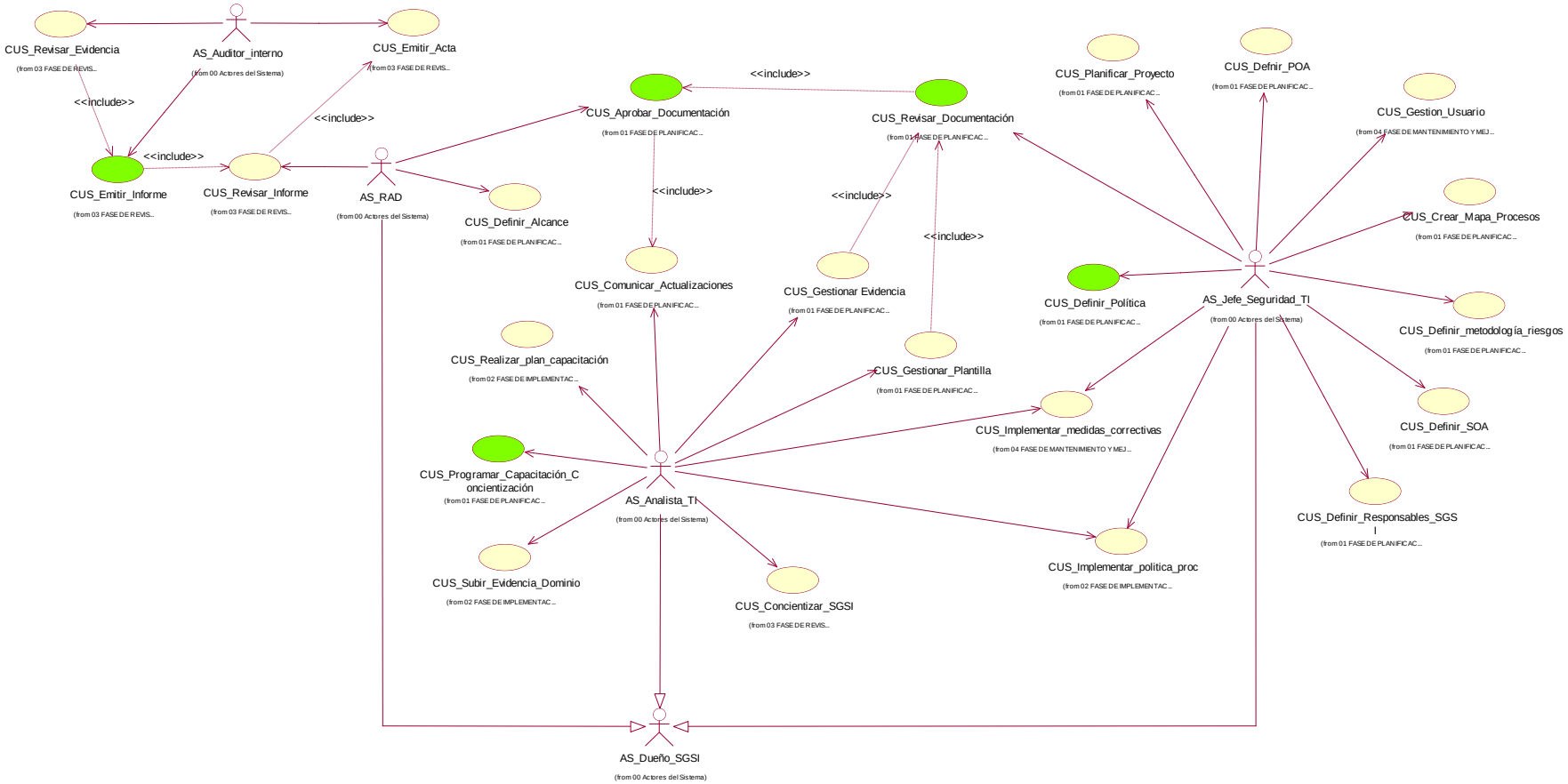


Figura N° 31 Diagrama CUS más significativos
Fuente: Elaboración Propia

Leyenda:
Color Verde: CUS más significativos del sistema.
Color Crema: CUS que guardan relación con los CUS más importantes.

4.4.2.2. Lista de Casos de usos más significativos

Tabla 57: Lista de Casos de usos más significativos

Módulo	Casos de Uso
Planificación	Aprobar documentación
	Crear mapa procesos
	Definir alcance
	Definir metodología de riesgos
	Definir política
	Definir responsables SGSI
	Definir SOA
	Definir POA
	Programar capacitación
	Revisar documentación
Implementación	Implementar política procedimiento
	Realizar plan capacitación
	Subir evidencia dominio
Revisión	Emitir Acta
	Emitir informe
	Revisar evidencia
	Revisar informe
Mantenimiento y mejora	Implementar medidas correctivas
	Gestionar usuario

Fuente: Elaboración Propia

En la tabla precedente (Ver tabla 57) se presentan los casos de uso más significativos para el sistema.

4.4.3. Vista lógica

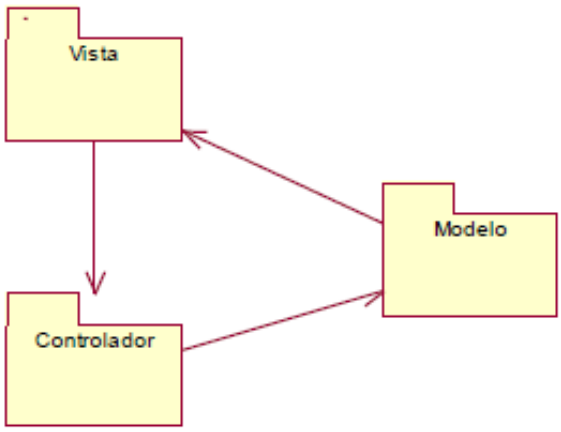


Figura N° 32 Vista lógica según MVC
Fuente: Elaboración propia

Para la realización del presente proyecto, se utilizó el modelo de vista controlador (MVC) el cual es un estilo de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario y la lógica de control en 3 componentes distintos (Ver figura N° 32).

4.4.4. Vista de implementación

El diseño de la solución y de los componentes de la misma se realizó teniendo en cuenta la base de datos, los frameworks y los principales paquetes de casos de uso ya mencionados anteriormente (Ver Figura N° 33).

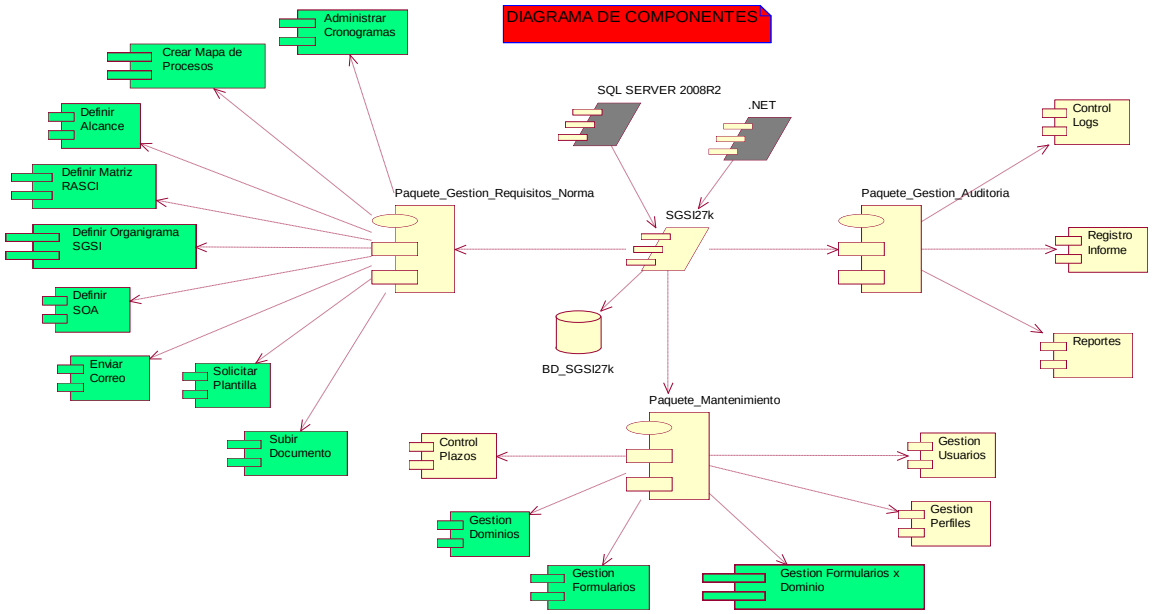


Figura N° 33 Diagrama de actores del sistema
Fuente: Elaboración propia

4.4.5. Vista de despliegue

4.4.5.1. Diagrama de despliegue: en el cual se modeló la arquitectura de la ejecución del sistema, y se muestran la relación que existen entre sus componentes (Ver Figura N° 34).

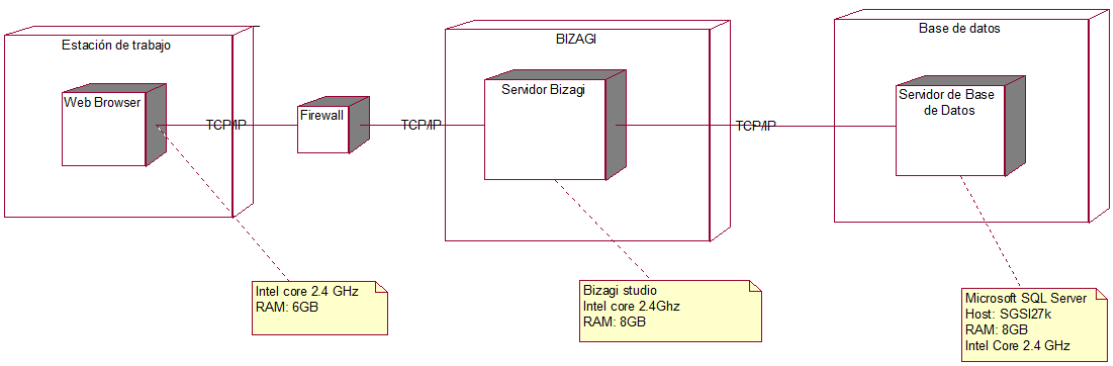


Figura N° 34 Diagrama de despliegue
Fuente: Elaboración propia

4.4.6. Vista de datos

4.4.6.1. Modelo físico de datos

Ver capítulo 4.3.4.2.

4.5. PRUEBAS

4.5.1. Plan de Pruebas

El objetivo del plan de pruebas es verificar que el sistema cumpla las necesidades establecidas por el usuario. A continuación (Ver Tabla 58), describiremos cada columna de la tabla.

- Fase del proceso (según ciclo de Deming): Plnf (Planificación), Implnt (Implementación), Rvsn (Revisión) y MntMj (Mantenimiento y mejora).
- Descripción: Es la descripción de lo que se quiere probar respecto al artefacto en el contexto del sistema.
- Resultado esperado: Es el resultado que se espera por el tester.
- Estado de Prueba: Finalizado, Probado y Falta.
- Tipo de Error: Sin Error, De Detalle, Leve y Grave.
- Tester: Es la persona que realiza las pruebas.
- Detalle de los Resultados: Es el resultado de la prueba realizada por el tester.

Tabla 58: Plan de pruebas

N°.	Fase	Unidad de Prueba	Descripción	Fecha planificada	Tester	Responsable
1	Plnf	Revisar documentación	Este caso de uso lo realiza el RAD, éste tiene que verificar la documentación que el jefe de seguridad ingresa (Documento).	01/09/2019	Paola	Keyla
2	Implnt	Subir evidencia	Este caso de uso lo realiza el analista. Este sube la documentación requerida de cada control.	10/09/2019	Paola	Keyla
3	Rvsn	Revisar informe preliminar	Este caso es realizado por el RAD, éste tiene que revisar el informe emitido por el auditor.	12/10/2019	Paola	Keyla
4	MntMj	Implementar medidas correctivas	Este caso es realizado por el jefe de seguridad y el analista. Después de que el auditor emitió el informe con los hallazgos, estas deben ser levantadas.	18/10/2019	Paola	Keyla

Fuente: Elaboración propia

4.5.2. Informe de pruebas.

El informe de pruebas de los casos de uso se muestra en las siguientes tablas (Ver tablas 59 y 62).

Tabla 59: Plan de prueba "CUS_ Revisar_Documentación"

Informe de prueba					
Unidad de Prueba:	CUS_Revisar_Documentación				
	Escenarios probados:				
Fecha:	01/09/2019		**Avance %**	100%	
Tester:	Paola Granados y Keyla Perez				
Descripción de la Prueba:	El objetivo de esta prueba es verificar que el RAD pueda verificar la documentación, para esto se tiene que mostrar la documentación ingresada por el jefe de seguridad.				
N°.	**Descripción**	**Acción**	**Resultado Esperado**	**Resultado**	**Detalle de los resultados**
1	Se abre la ventana de "Evaluar contenido" y se debe mostrar el contenido del formulario con los datos registrados por el jefe de seguridad.	Ver datos registrados	Se espera que se muestren los datos registrados.	Si Pasó	Al ingresar a la ventana, se muestran todos los datos registrados.
2	El documento se debe poder generar con todos los datos correctos del registro.	Generación del documento correctamente	Se espera que el documento que se genere esté con todos los datos que se registraron.	Parcial	Al dar clic en el botón "Generar documento", se genera el documento con todos los datos, pero la fecha de la versión y el nivel de confidencialidad del documento no son correcta.

Fuente: Elaboración propia

Tabla 60: Plan de prueba “Subir evidencia dominio”

Informe de prueba					
Unidad de Prueba:	CUS_ Subir_evidencia_dominio				
	Escenarios probados:				
Fecha:	10/09/2019		**Avance %**	100%	
Tester:	Paola Granados y Keyla Perez				
Descripción de la Prueba:	El objetivo de esta prueba es verificar que el jefe de seguridad pueda subir las evidencias que se requieren en cada dominio.				
N°.	**Descripción**	**Acción**	**Resultado Esperado**	**Resultado**	**Detalle de los resultados**
1	Se abre la ventana de “Subir evidencia” y se debe mostrar el contenido del formulario con la descripción del control.	Ver datos registrados	Se espera que muestre los datos del control	Si Pasó	Al ingresar a la ventana, se muestre la descripción del control.
2	Al subir la evidencia, debe validar que permita subir la cantidad máxima de archivos especificados.	Subir archivos	Se espera la validación de cantidad máxima de archivos permitidos.	Si Pasó	Al subir documentos, me muestra un mensaje de error si es que pasó de la cantidad máxima de archivos.
3	Al subir la evidencia, debe validar tipo de extensión permitido.	Subir archivos	Se espera la validación del tipo de extensión	Si Pasó	Al subir documentos, me muestra un mensaje de error si es que subo otro tipo de extensión especificada.

Fuente: Elaboración propia

Tabla 61: Plan de prueba “Revisar informe preliminar”

Informe de prueba					
Unidad de Prueba:	CUS_ Revisar_Informe				
	Escenarios probados:				
Fecha:	12/10/2019		**Avance %**	100%	
Tester:	Paola Granados y Keyla Perez				
Descripción de la Prueba:	El objetivo de esta prueba es que el RAD pueda revisar el informe preliminar emitido.				
N°.	**Descripción**	**Acción**	**Resultado Esperado**	**Resultado**	**Detalle de los resultados**
1	Al abrir la venta de revisión, se debe mostrar el formulario del informe con todos los datos registrados por el auditor.	Ver datos del informe	Se espera que muestre todos los datos del informe.	Si Pasó	Al ingresar a la ventana, se muestran todos los datos.
2	Al abrir la venta de revisión, se debe mostrar el historial de cambios del informe de revisión.	Ver datos del historial	Se espera que se muestre el historial de cambios	Parcial	Al ingresa a la ventana, me muestra el historial de cambios, pero no me indica quién lo realizó.

Fuente: Elaboración propia

Tabla 62: Plan de prueba “Implementar medidas correctivas”

Informe de prueba					
Unidad de Prueba:	CUS_ Medidas_Correctivas				
	Escenarios probados:				
Fecha:	18/10/2019		**Avance %**	100%	
Tester:	Paola Granados y Keyla Perez				
Descripción de la Prueba:	El objetivo de esta prueba es que el RAD pueda revisar el informe preliminar emitido.				
N°.	**Descripción**	**Acción**	**Resultado Esperado**	**Resultado**	**Detalle de los resultados**
1	Al abrir la ventana, me debe mostrar la lista de los hallazgos emitida en el informe del auditor.	Ver datos de los hallazgos.	Se espera que muestre todos los hallazgos	Si Pasó	Al ingresar a la ventana, se muestran todos los datos.
2	Al hacer clic en cada hallazgo, me debe mostrar las causas de cada hallazgo.	Ver datos del hallazgo	Se espera que se muestre las causas de los hallazgos.	Si Pasó	Al hacer clic en cada hallazgo, me muestra las causas.
3	Al ingresar a la ventana de ejecución de plan de acción, me debe mostrar las actividades del plan de acción.	Ver datos del plan de acción	Se espera que se muestre los datos del plan de acción	Si Pasó	Al ingresar a la ventana, se muestra las actividades del plan de acción.
4	Al ingresar a la ventana de verificación de resultados, me debe mostrar los resultados que se obtuvieron al implementar el plan de acción.	Ver datos de los resultados	Se espera que se muestre todos los resultados de la ejecución del plan de acción.	Si pasó.	Al ingresar a la ventana, se muestra todos los resultados de la implementación del plan de acción.

Fuente: Elaboración propia

4.5.3. Manual de Implementación

4.5.3.1. Manual de Configuración

Ver ANEXO 1 – Manual de Configuración

4.5.3.2. Manual de Usuario

Ver ANEXO 2 – Manual de Usuario

CONCLUSIONES

Durante la etapa de elaboración del proyecto, se ha llegado a las siguientes conclusiones:

1) El contar con un sistema que ayuda a seguir las buenas prácticas en seguridad de la información, alineado a la ISO 27001, es importante para industrias Triveca ya que ayuda a controlar adecuadamente los activos de información.

2) Definir políticas y procedimientos alineados al sistema de gestión de seguridad de información, nos permitió conocer mejor el flujo de trabajo de industrias Triveca y a la par poder ayudar a prevenir posibles incidentes de seguridad de información.

3) Durante la realización del presente trabajo, se pudo validar la falta de conocimiento de seguridad de información de los colaboradores de industrias Triveca, dejando vulnerable a la compañía ante los posibles riesgos de seguridad de información vital para su funcionamiento.

4) Si bien no se encuentra dentro del alcance la realización de un análisis de riesgos a profundidad en industrias Triveca, si se otorgan las pautas y los formatos para la clasificación de activos (tecnológicos y de información) de acuerdo a su nivel de importancia, ya que ello ayuda a evaluar el nivel de riesgo involucrado para controlarlo a través de un plan de acción.

RECOMENDACIONES

Durante la etapa de elaboración del proyecto, se ha llegado a las siguientes recomendaciones.

1) Se ha demostrado que si bien el sistema ayuda a las buenas prácticas en seguridad de información, no es posible si no se tiene apoyo de la alta dirección en cuanto a capacitaciones y concientización a los colaboradores internos.

2) Para evitar algún error o fallo en el uso del sistema se sugiere utilizar equipos o dispositivos que cuenten con los requisitos recomendados.

3) Se debe tener en consideración que es importante capacitar y/o concientizar a los colaboradores en temas referentes a seguridad de información.

4) Muchas compañías tienen políticas básicas de seguridad, pero muy pocas implementan una cultura de conciencia de seguridad que fomente a que el colaborador cuide su información y el de la compañía y más aún no se alinean a ningún estándar de seguridad es por ello que recomendamos a las ISO 27001 como un conjunto de buenas prácticas.

5) Existen departamentos que no fueron contemplados en el presente proyecto, por lo que se debe considerar en un futuro la integración y mejora en seguridad de información de toda la compañía.

6) Si bien sólo se ha considerado en el proyecto la prueba del sistema en dos dominios del anexo A de la 27001, se debe tomar en cuenta que para un futuro se debe considerar los 14 dominios ya que protegen la información en todos los aspectos.

REFERENCIAS BIBLIOGRÁFICAS

Barragán, I., Góngora, I., & Ericka, M. (2011). *Implementación de políticas de seguridad informática para la m.i. municipalidad de Guayaquil aplicando la norma iso/iec 27002.* (Tesis de pregrado), Universidad Ricardo Palma, Lima - Perú Obtenido de http://cybertesis.urp.edu.pe/urp/2007/munoz_ef/pdf/munoz_ef-TH.3.pdf

Cuatrecasas, L. (2010). *Gestión Integral de la Calidad.* BRESCA (PROFIT EDITORIAL).

Educaplus. (26 de junio de 2017). *Latitud y longitud | Educaplus*. Obtenido de Educaplus - Recursos educativos para la enseñanza de las ciencias: http://www.educaplus.org/game/latitud-y-longitud

García Moreno, M. (1999). *Gestión del conocimiento en las organizaciones a través del workflow.* Obtenido de El profesional de la información.

García Moreno, M. A. (1999). *CALIDAD TOTAL Y WORKFLOW: UN NUEVO RETO.*

Globalsuite. (2016). *globalsuite.es*. Obtenido de https://www.globalsuite.es

Gómez Fernández, L., & Andrés Álvarez, A. (26 de junio de (2009)). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* España: AENOR Ediciones(Asociación Española de Normalización). Obtenido de Alegsa.com.ar - Portal de informática, tecnologías y web: http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf

González Lorca, J. (2006). *Sistemas workflow, Funcionamiento y metodología de implantación.* España: Ediciones Trea.

González Trejo, D. (2013). *ISO-27001:2013 ¿Qué hay de nuevo?* Obtenido de magazCitum: https://www.magazcitum.com.mx/?p=2397#.XRhTU-tKjIU

Informática hoy. (26 de junio de 2017). *Qué es el GPS y cómo funciona*. Obtenido de Informática y tecnología sin complicaciones: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-el-GPS-y-como-funciona.php

ISO 27000.es. (2012). *Ciclo Deming (2005)- mejora continua*. Obtenido de ISO 27000.es: http://www.iso27000.es/sgsi_implantar.html

ISO/IEC 27001. (2005). *Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la información - Requisitos.*Suiza: AENOR.

ISO/IEC 27001. (2013). *Tecnología de la Información – Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la información - Requisitos.* Suiza: AENOR.

Jaferian, P., Hawkey, K., Sotirakopoulos, A., Velez-Rojas, M., & Beznosov, K. (2011). *Heuristics for evaluating IT security management tools.* HCI Editorial Record.

KOTLER, P., & KELLER, K. L. (2012). *Dirección de marketing.* Mexico: Pearson.

La real Academia Española. (2012). *RAE*. Obtenido de http://lema.rae.es/drae/?val=sistemas

Lisot. (2019). *¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)?* Obtenido de https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

Merino Bada, C., & Cañizares Sales, R. (2011). *Implantación de un Sistema de Gestión de seguridad de la Información según ISO 27001: Un enfoque práctico.* FC EDITORIAL.

meycor. (2015). *meycor-soft*. Obtenido de http://www.meycor-soft.com/es

NovaSec. (2015). *Novasec*. Obtenido de http://www.novasec.co/",

Saberi, I., Federrath , H., & Shojaie, B. (2014). *Evaluating the effectiveness of ISO 27001:2013 based on Annex A.* Suiza. Recuperado el 10 de 05 de 2015

Saberi, I., Federrath, H., & Shojaie, B. (2014). *Evaluating the effectiveness of ISO 27001:2013 based on Annex A.*

Universidad Santo Tomás. (26 de junio de 2017). *Soporte a Servidores*. Obtenido de Inicio: http://www.ustamed.edu.co/sistemas/index.php/frentes/sistemas/soporte-a-servidores

ANEXO 1

1. MANUAL DE CONFIGURACIÓN

Contenido

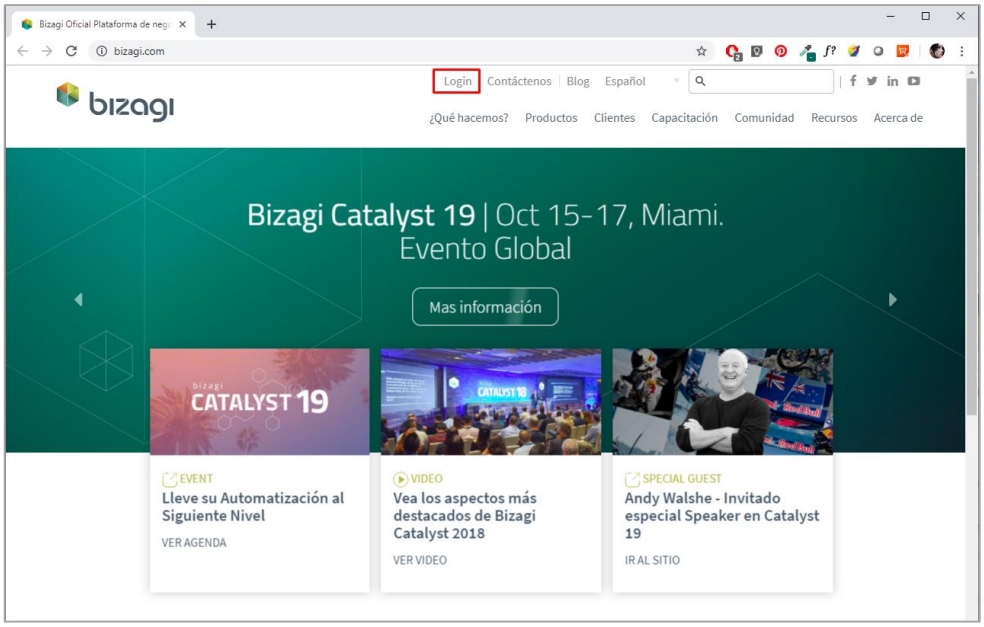
1. Instalación de Bizagi Studio en Windows
2. Instalación y configuración para el trabajo colaborativo
3. Seguridad de Bizagi Studio
4. Configuración de entornos

1. Instalación de Bizagi Studio en Windows

1.1. Descarga

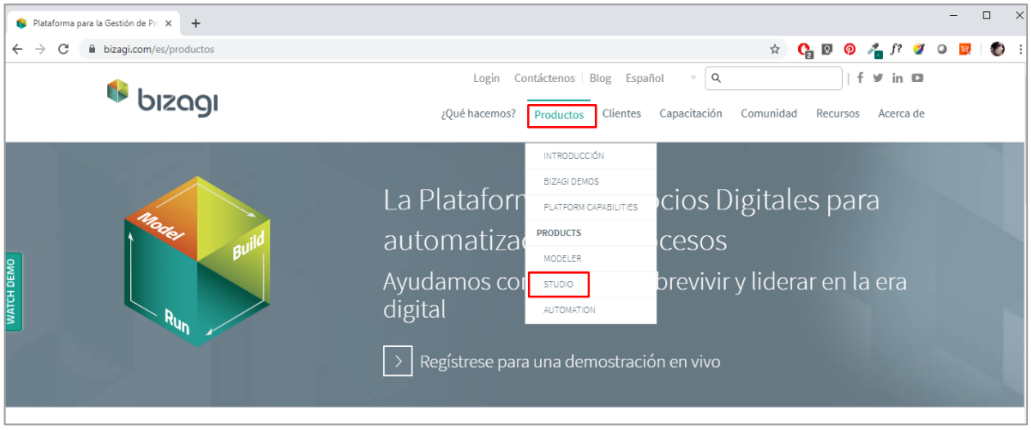
Este proceso describe los pasos de la descarga e instalación de Bizagi Studio, para esto se requiere que el usuario tenga una cuenta en Bizagi para que permita la descarga.
A continuación, detallamos los pasos a seguir.

a) Ingrese a la página de Bizagi (Bizagi.com) y haga clic en “Login”.

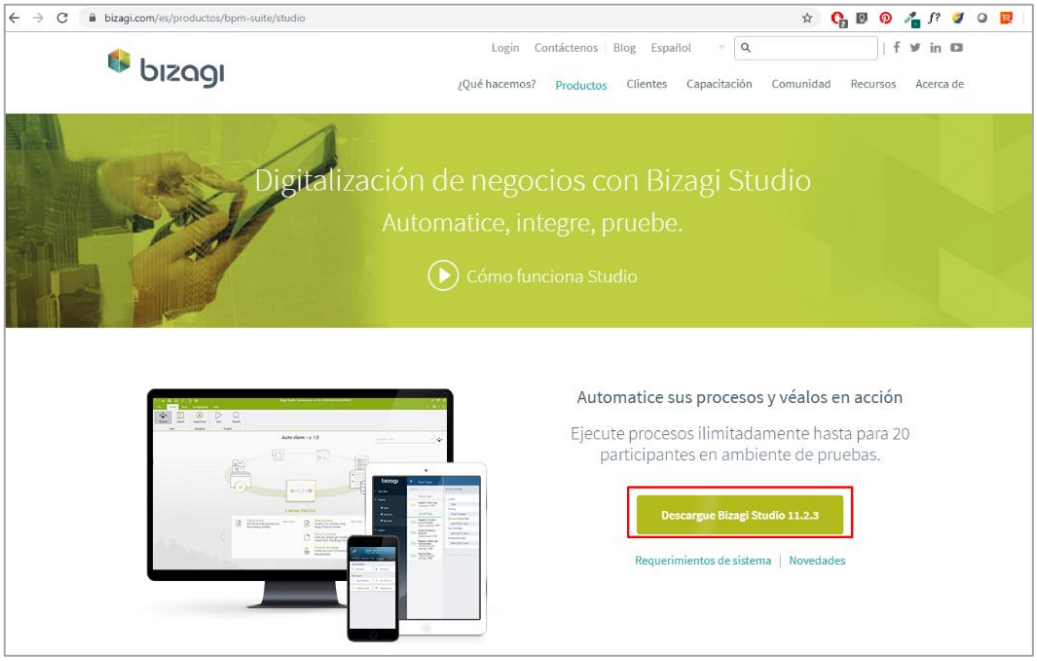


b) Si es que no tiene una cuenta en Bizagi, proceda a registrarse o si es que tiene, inicie sesión.

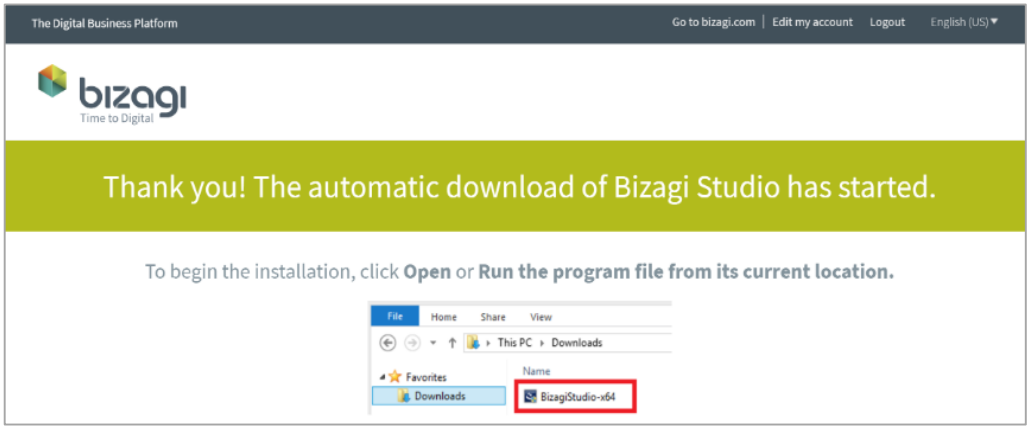
c) Una vez ingresó al portal de Bizagi, de clic en **Productos > Studio**



d) Desplácese hacia abajo y haga clic en el botón de descarga

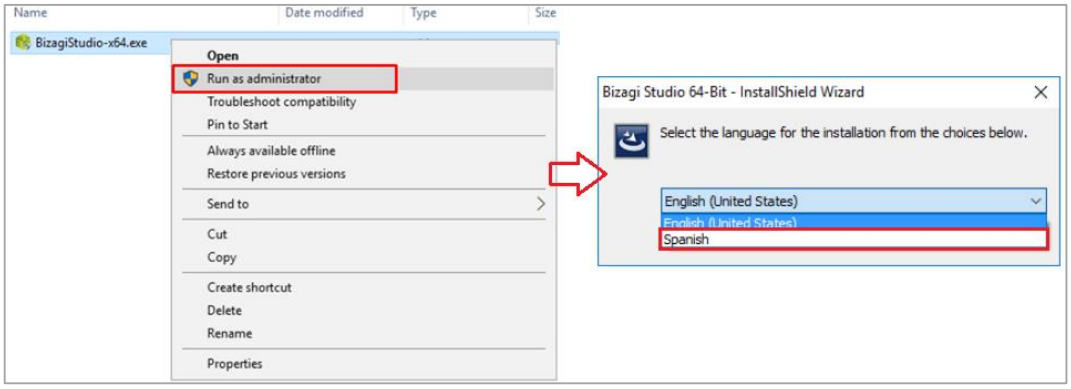


La descarga empezará automáticamente

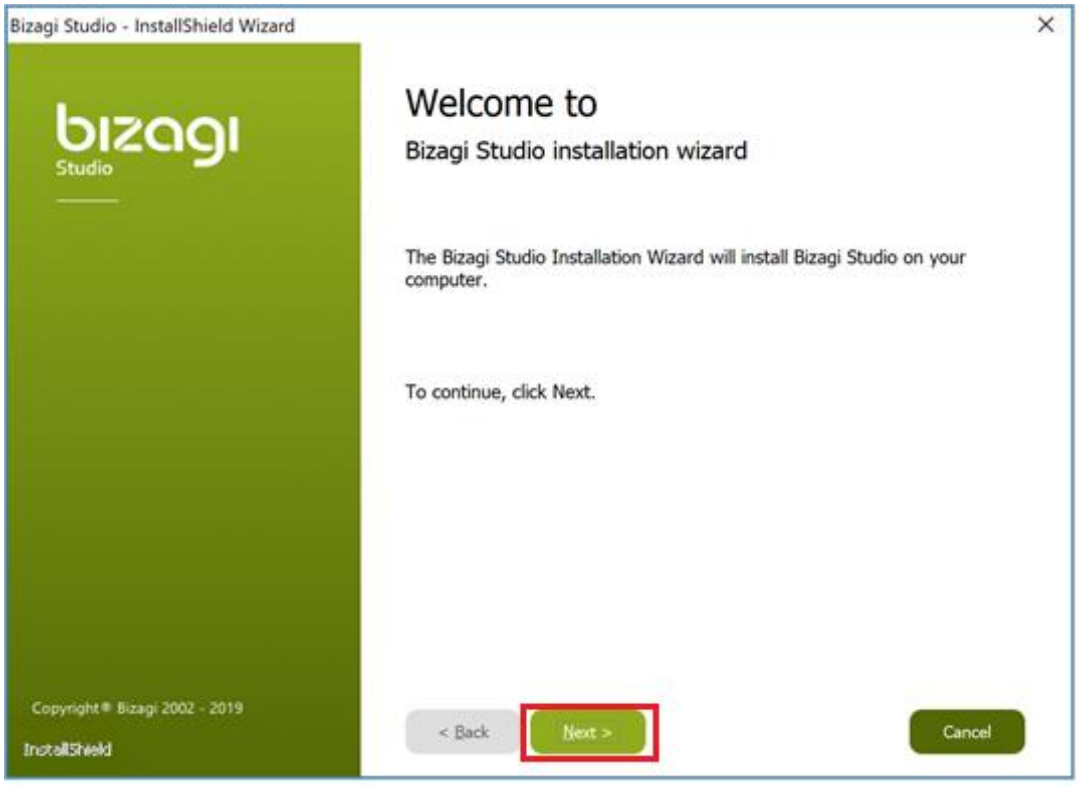


1.2. Instalación

a) Una vez descargado el instalador, ejecútelo con permisos de administrador y selecciones el idioma para la instalación.

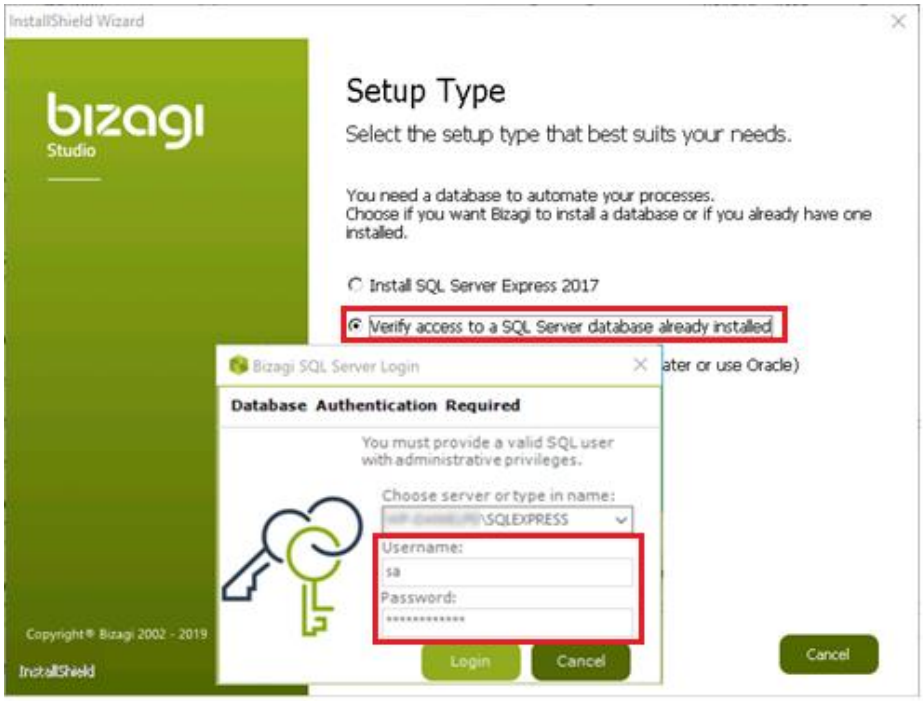


b) Cuando la ventana de Bienvenida se abra, dé clic en **siguiente**

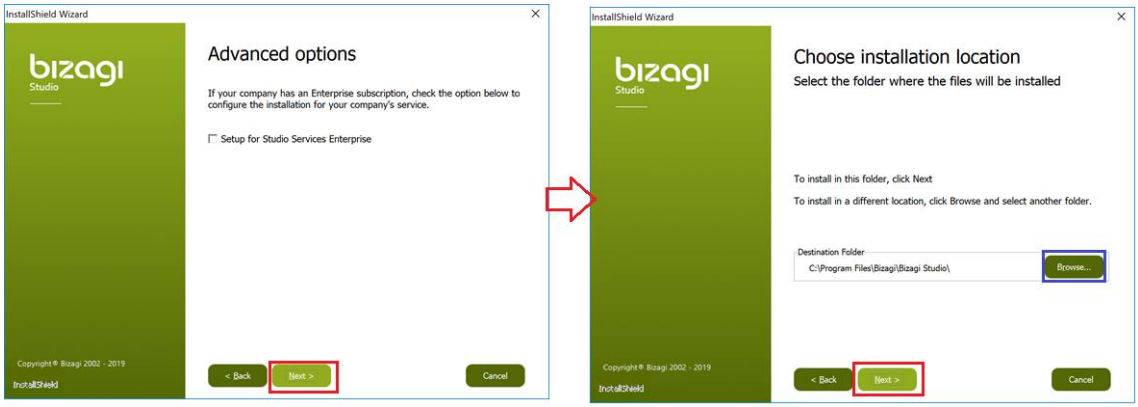


c) Acepte los términos de licencia y dé clic en **siguiente**.

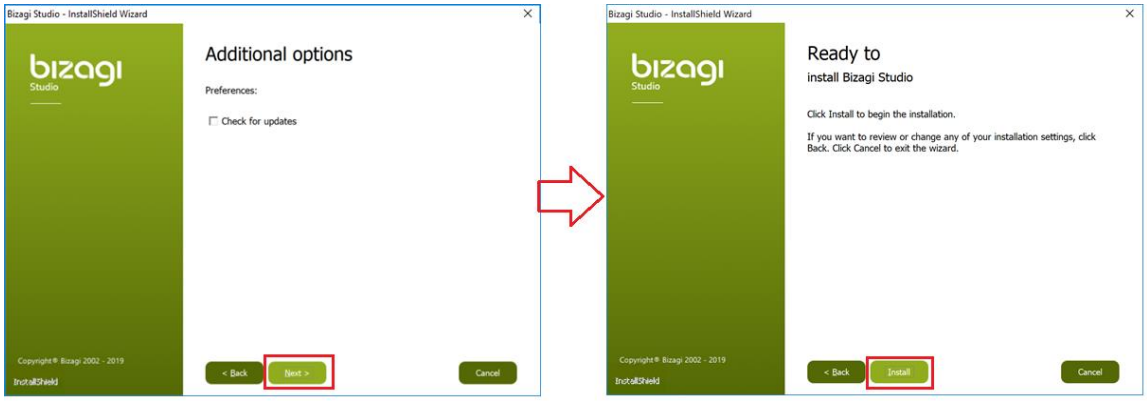
d) Para este punto, como requisito del sistema se solicitó que ya se tenga SQL server instalado. Seleccione la opción **"Comprobar acceso a una base de datos SQL Server ya instalada".** Ingrese el usuario (sa) y contraseña para la autenticación de SQL server. Una vez ingresada los datos requeridos, de clic en **Login** para verificar la conexión.



e) Dé clic en siguiente, Si deseas que Bizagi se instale en la ruta predeterminas. De lo contrario haz clic en Buscar y seleccionar la carpeta que deseas.

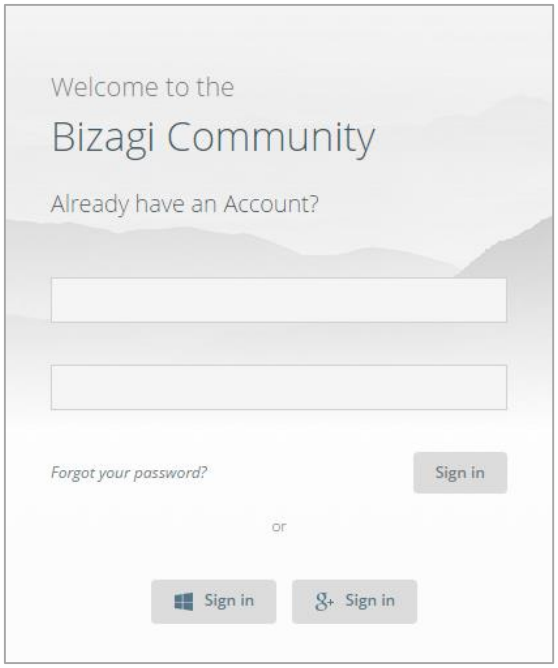


f) De clic en siguiente, si marca la casilla éste va a ***Comprobar si hay actualizaciones.*** En la siguiente ventana, haga clic en **Instalar** para comenzar con la instalación.



g) La siguiente ventana aparecerá cuando la instalación haya terminado. Dé clic en **Finalizar**. Se requiere el reinicio del equipo para su correcto funcionamiento

h) Al iniciar el Bizagi Studio, aparecerá una ventana donde debe ingresar sus credenciales de la cuenta www.bizagi.com. De esta manera se beneficiará de los recursos gratuitos y el soporte que ofrece Bizagi.



2. Instalación y configuración para el trabajo colaborativo

A través de lo que ofrece Bizagi Studio como herramienta para el trabajo colaborativo, éste se instala tanto en el servidor en el que se encuentra el proyecto y en las estaciones de trabajo que se conectan al proyecto remoto.
Como requerimiento, se necesita que haya conexión de red entre las estaciones de trabajo y el servidor central.

Requerimientos técnicos

Tabla Requerimiento técnicos para el trabajo colaborativo

Tipo de puerto	Número de puerto	Para comunicación entre
TCP	5679	- Las estaciones de los desarrolladores que utilizan Bizagi Studio y el servidor de Desarrollo que utiliza Bizagi Studio.
TCP	Como se definió para el servicio de su instancia de base de datos (por ejemplo, 1433 es el puerto predeterminado para SQL Server y 1521 es el puerto predeterminado para Oracle).	- Las estaciones de los desarrolladores que utilizan Bizagi Studio y el servidor de Base de Datos. Esta conexión es cifrada - El servidor de Desarrollo que utiliza Bizagi Studio y el servidor de Base de Datos.

TCP	Usualmente el puerto 80 para HTTP (o el puerto 443 para HTTPS)	- Las estaciones de los desarrolladores que utilizan Bizagi Studio y el servidor de Desarrollo que utiliza Bizagi Studio.

Fuente: http://help.bizagi.com/bpm-suite/es/index.html?studio_teamwork.htm

Ser requiere una cuenta de administrador local en el servidor de Desarrollo, éste se encargará de la administración del proyecto de Bizagi. Los usuarios que trabajarán en el proyecto no necesitan que tengan permisos de administrador, pero sí deben estar autorizados en el grupo Bizagi.

A continuación, detallamos los pasos a seguir:

2.1. Instalar Bizagi Studio en el servidor central.

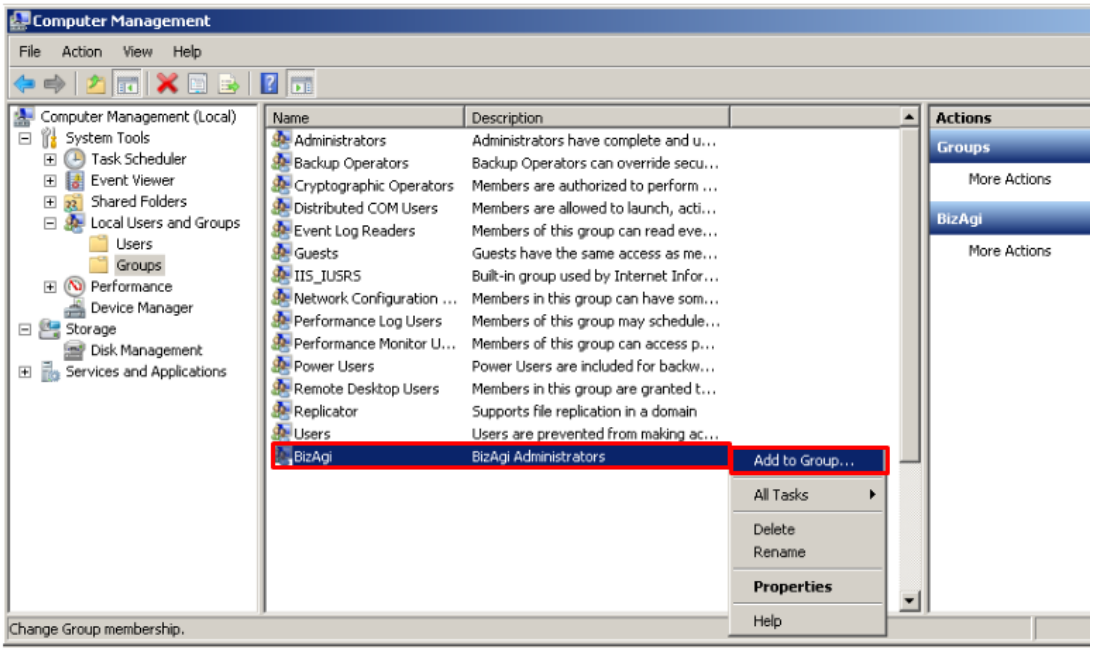
a. Instale Bizagi Studio ejecutando el instalador con derechos de administración en el servidor central.
b. Siga los pasos descritos en el punto 1 e ingrese las credenciales de su instancia corporativa de su servidor de base de datos. (Las credenciales de SQL se usarán desde las diferentes estaciones de trabajo que se conecten al servidor central)
c. Verifique su acceso.

2.2. Crear el proyecto Bizagi en el servidor central.

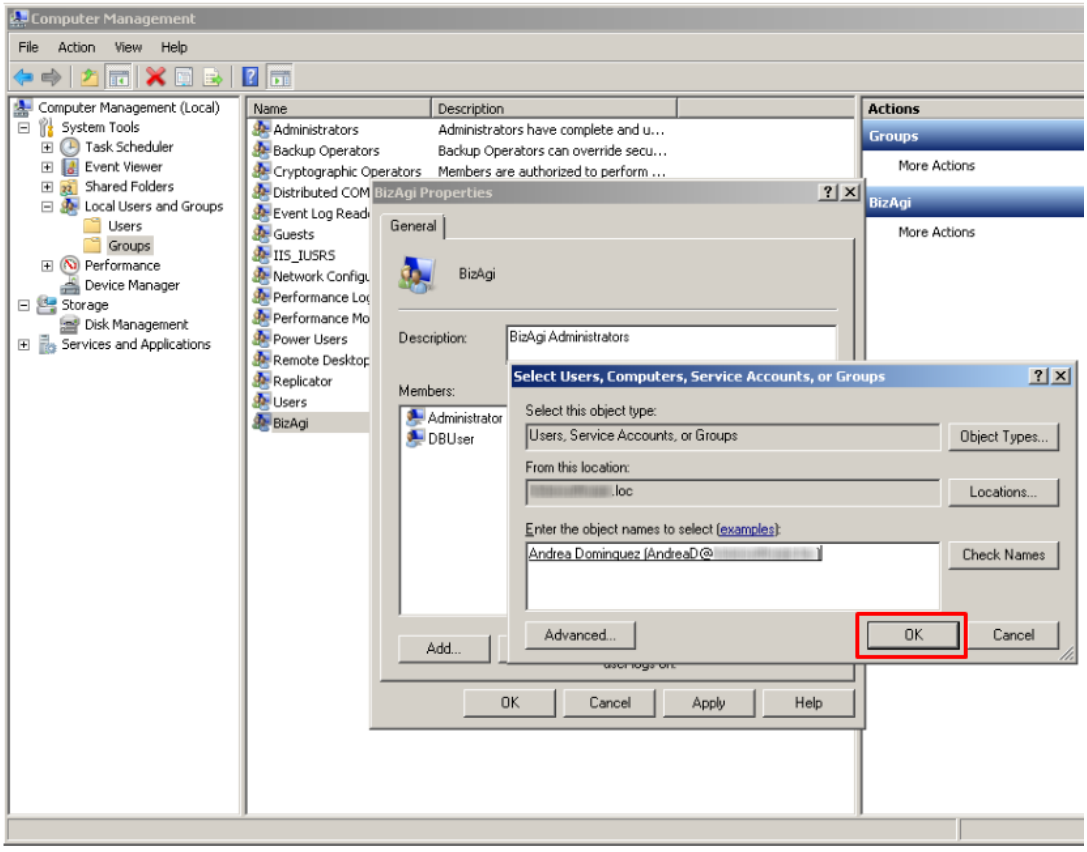
a. Cree un nuevo proyecto de Bizagi en el servidor central. (Desde la cuenta administrador)
b. Restaure la copia de seguridad de base de datos de su proyecto que quiere importar en el proyecto que acaba de crear.

2.3. Incluir los registros de autorización en el servidor central para los usuarios.

a. Ya en el servidor, agregue todas las cuentas de su equipo en el grupo Bizagi. (El grupo Bizagi de crea automáticamente durante la instalación e incluye al administrador local por defecto.)
b. Para añadir usuarios o grupos del directorio activo a este grupo (Bizagi), haga clic derecho en el grupo para utilizar la opción *Agregar al grupo:*



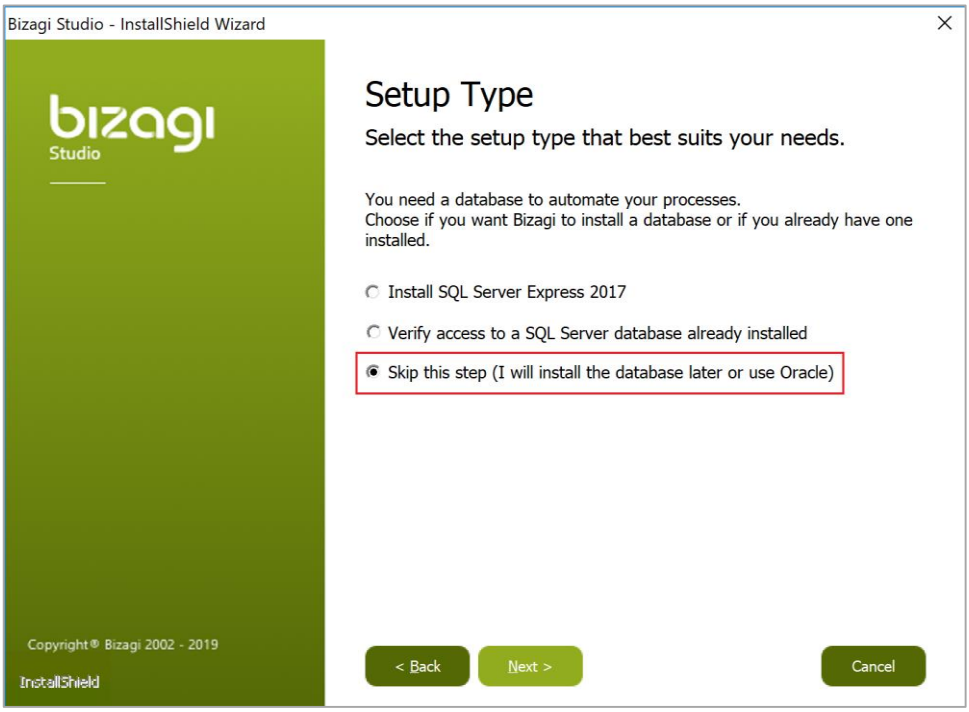
Escoja los usuarios o el grupo del directorio activo de desea que se conecten al proyecto.



2.4. Instalar Bizagi Studio en las estaciones de trabajo de los usuarios que se conectan a este proyecto.

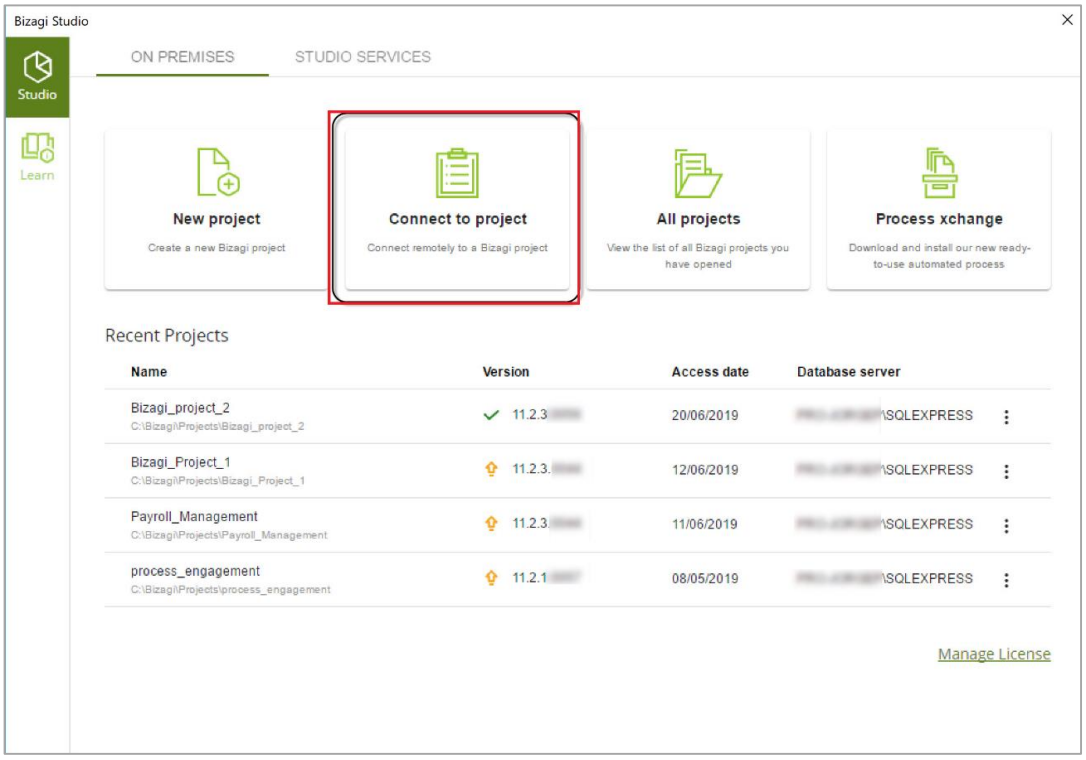
a) Instale Bizagi Studio (Siga los pasos descritos en el punto 1) en las estaciones de trabajo del equipo. (La versión de Bizagi que se instale, debe ser la misma que se instaló en el servidor central)

b) En este punto al instalar Bizagi, debe omitir los pasos relacionados a la instancia de Base de datos, ya que utilizará el servidor central.

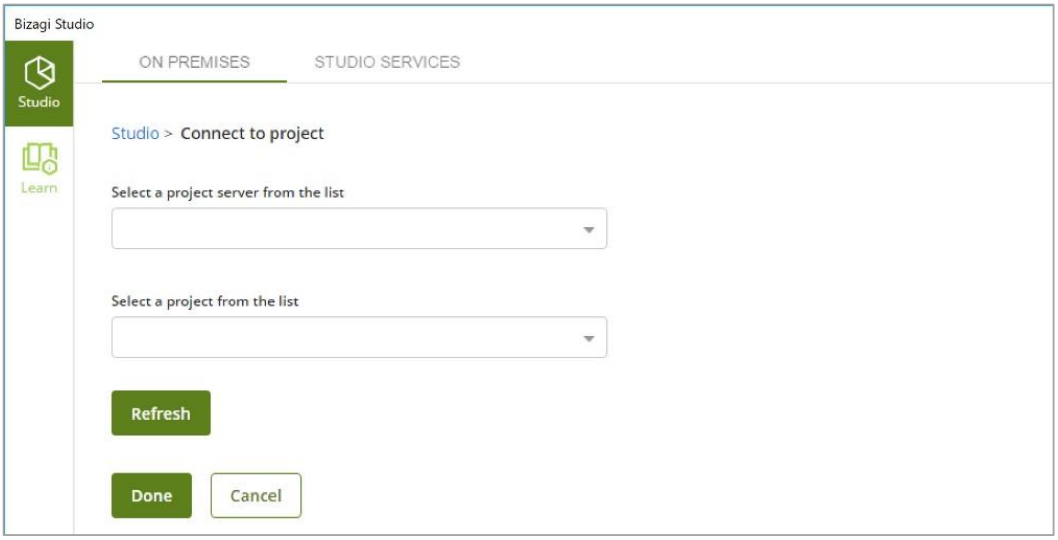


2.5. Conectarse al proyecto desde las estaciones de trabajo

a) Para conectarse al proyecto, abra Bizagi Studio y seleccione la opción **Abrir proyecto existente**.

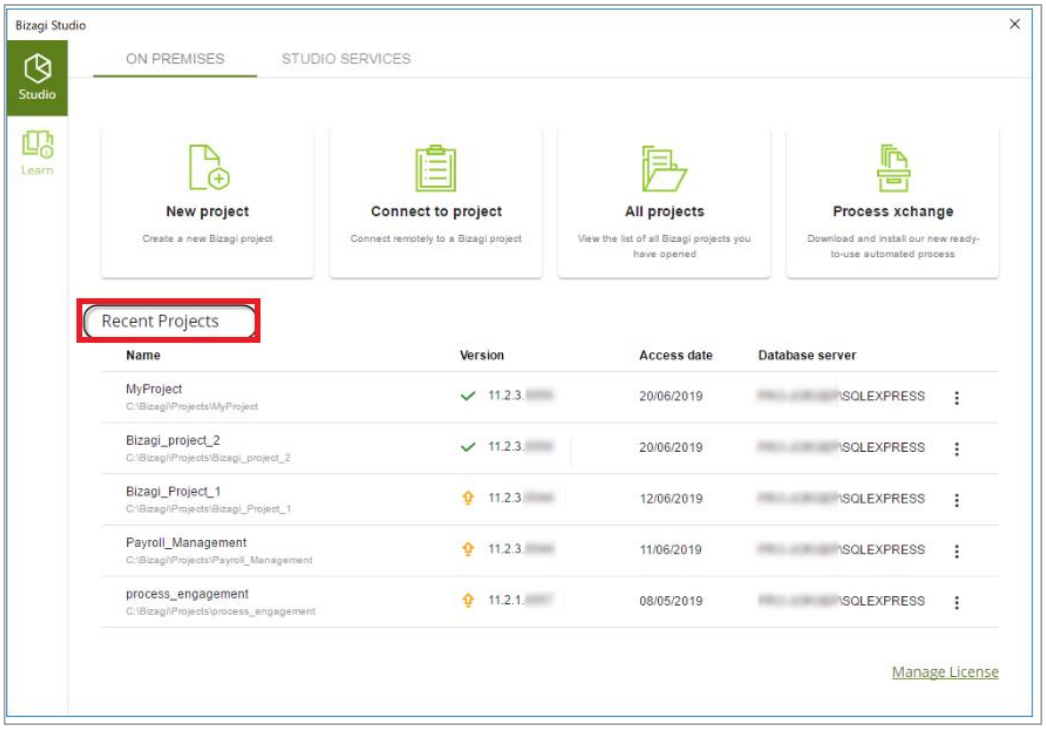


b) Seleccione el servidor central del proyecto y seleccione el proyecto. Dé clic en Finalizar.



c) Si el proyecto se cargó, entonces la configuración de acceso al proyecto ha sido correcta.

Terminado este punto, los usuarios podrán conectarse al proyecto fácilmente. Desde la ventana inicial de Bizagi se listarán todos los proyectos que han sido abiertos recientemente.



3. Seguridad de Bizagi Studio

En Bizagi se puede trabajar simultáneamente en el mismo proyecto, esto requiere por seguridad, que sea necesario restringir el acceso a algunos usuarios.

Inicialmente todos los proyectos de Bizagi se crean sin seguridad. Se puede gestionar la seguridad para las aplicaciones, procesos, Entidades y las reglas de negocio.

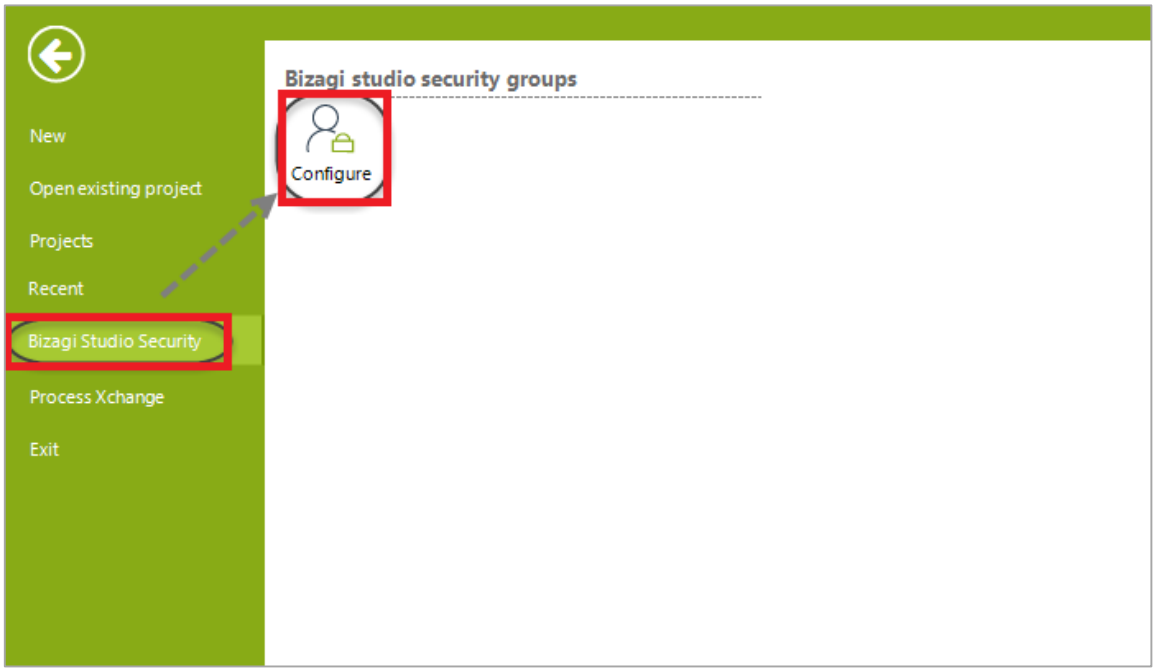
Para administrar los derechos de acceso en Bizagi Studio, se necesita habilitar la característica de seguridad y definir los permisos para cada elemento.

A continuación, detallamos los pasos a seguir.

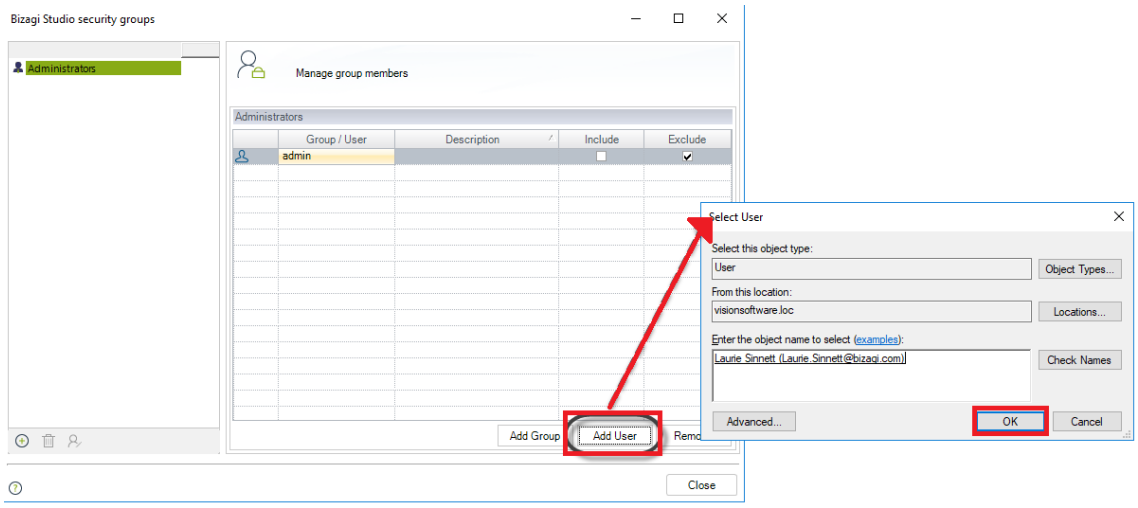
3.1. Habilitar la Seguridad de Bizagi Studio

a) Se debe definir uno o más administradores del proyecto, solo este perfil tendrá acceso y permiso a la configuración de seguridad de Bizagi.

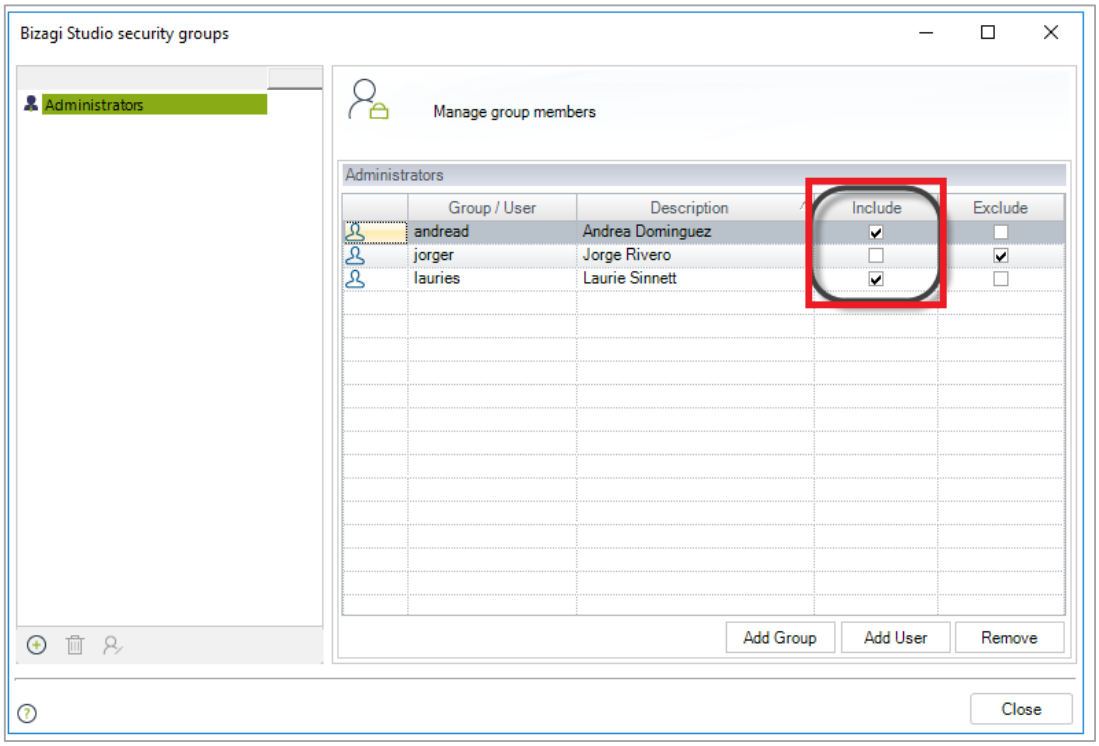
b) Para adicionar un administrador, haga clic en la **Vista de experto > Archivo > Seguridad de Bizagi Studio > Configurar.**



c) En la ventana, haz clic en **Agregar usuario** y seleccione el usuario. Sólo los usuarios que pertenecen al dominio donde se encuentra el proyecto se podrán incluir.



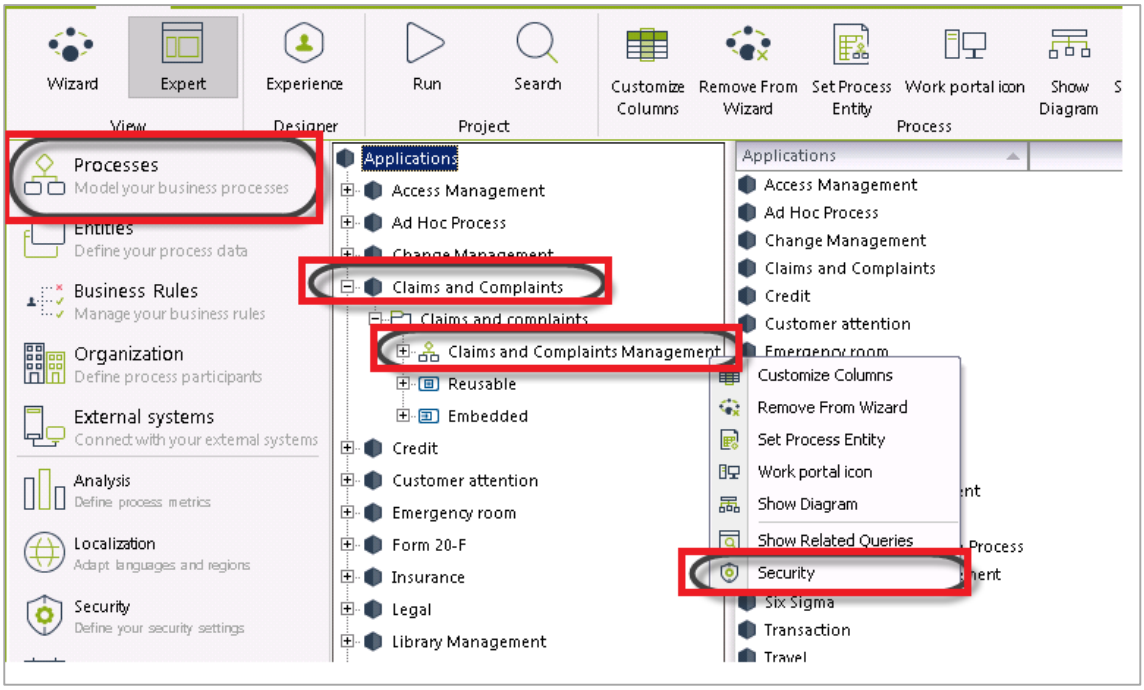
d) Puede incluir varios usuarios al grupo de administradores, para esto debe marcar la casilla Incluir para que estos usuarios sean administradores.



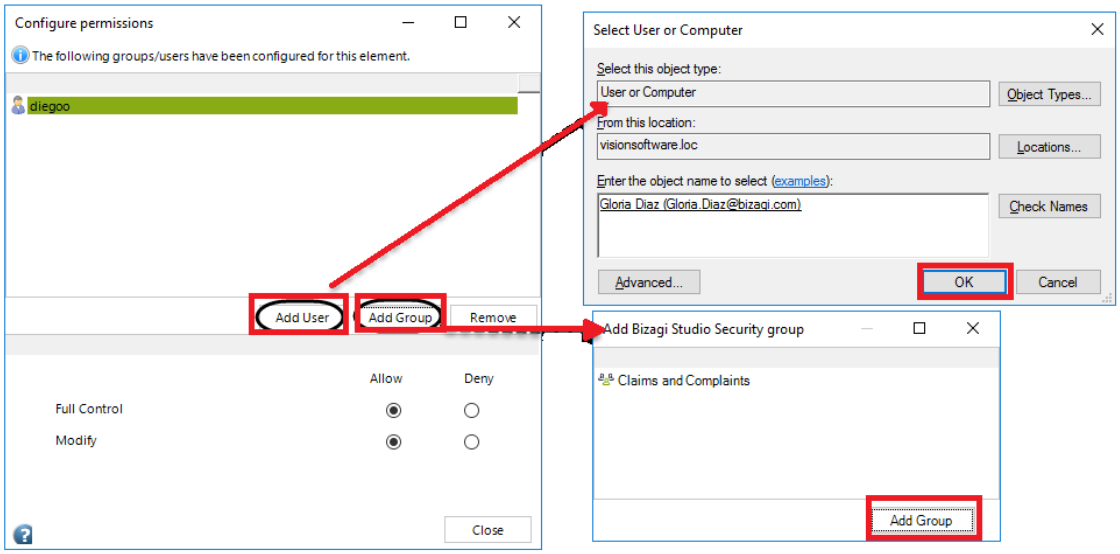
3.2. Conceder acceso a los recursos

Para conceder derechos de acceso debe ser un *Administrador* o tener permisos de *Control total* sobre el elemento.

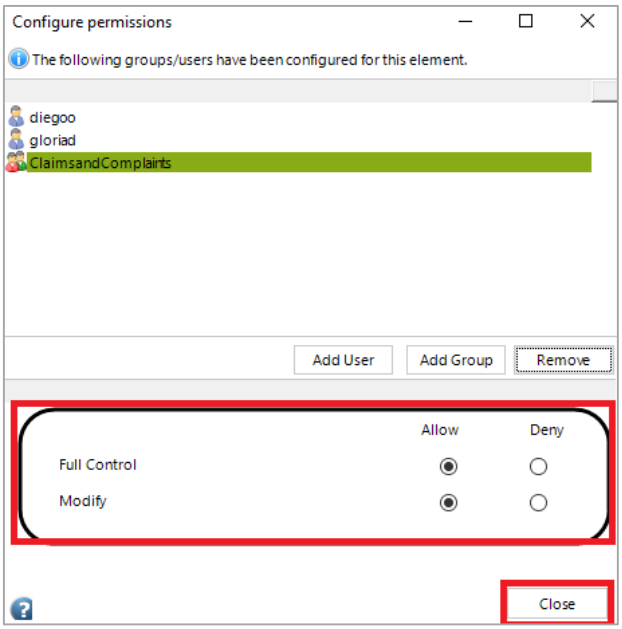
a) Daremos permiso de acceso a un proceso llamado *Quejas y Reclamos*. Haga clic en +, para desglosar la carpeta, haga clic derecho en Seguridad



b) En esta ventana puede administrar los permisos de los usuarios y grupos.

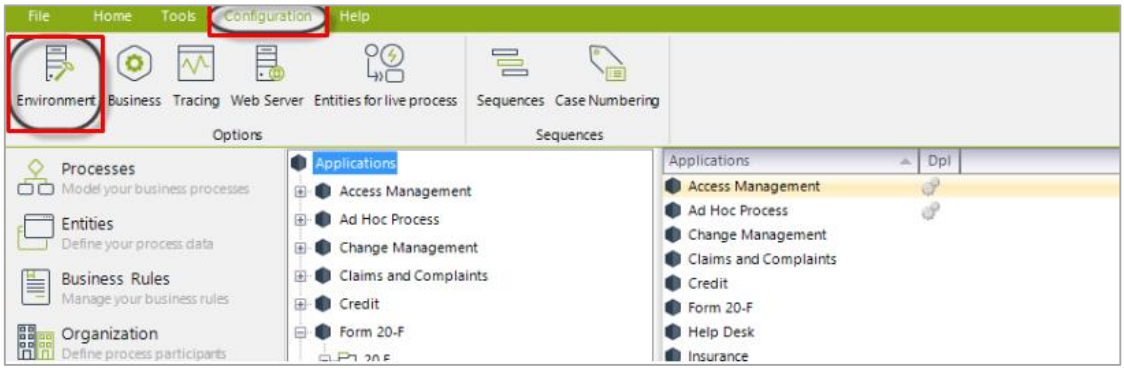


c) Dé los permisos de acceso que desee y cuando termine dé clic en cerrar.

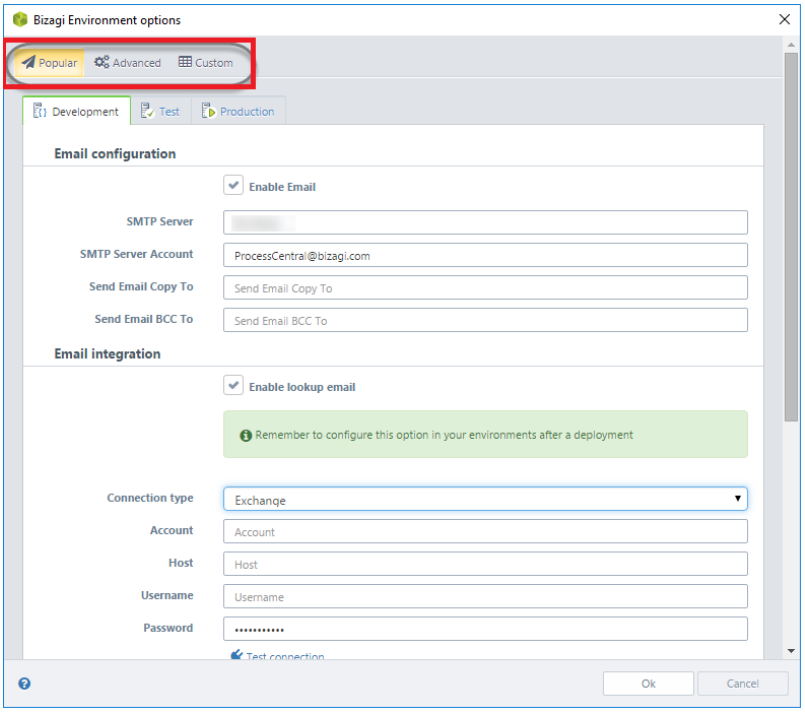


4. Configuración de entorno

La Configuración de Entorno especifica la configuración del envío de correos, Schedule y la autenticación. Para configurar el entorno tienes que ingresar a la pestaña Configuración > Entorno.

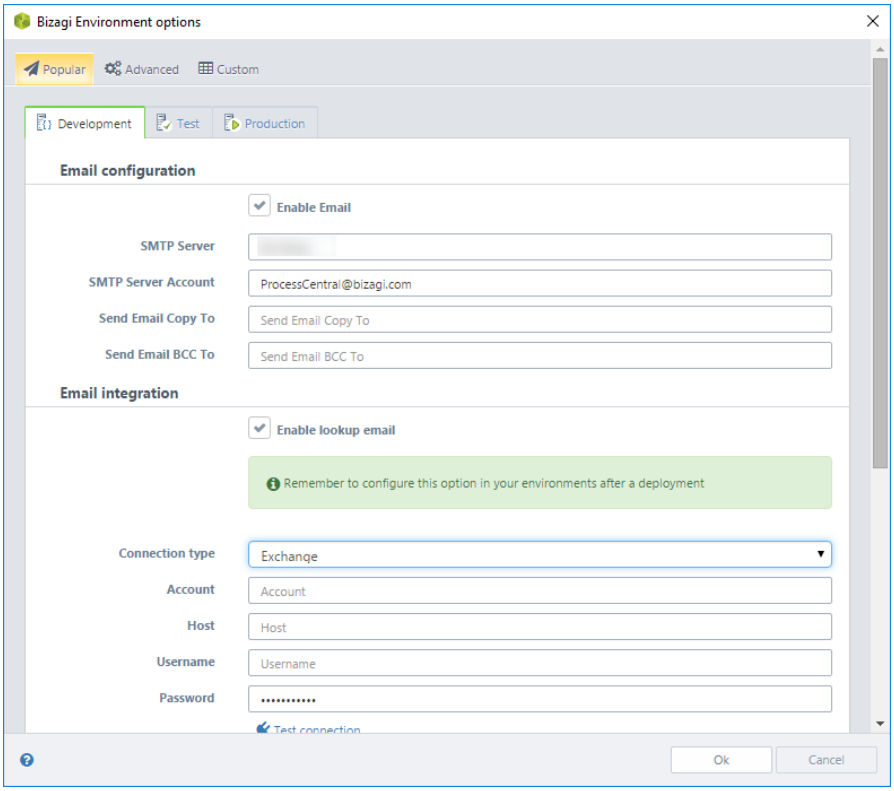


La figuración de entorno posee tres opciones: Popular, Avanzado y Personalizado



4.1.Popular

Aquí se configura los parámetros para envío de correo electrónico en los ambiente (desarrollo, Test, producción).



Los parámetros para configurar son:

Tabla Parámetros de configuración

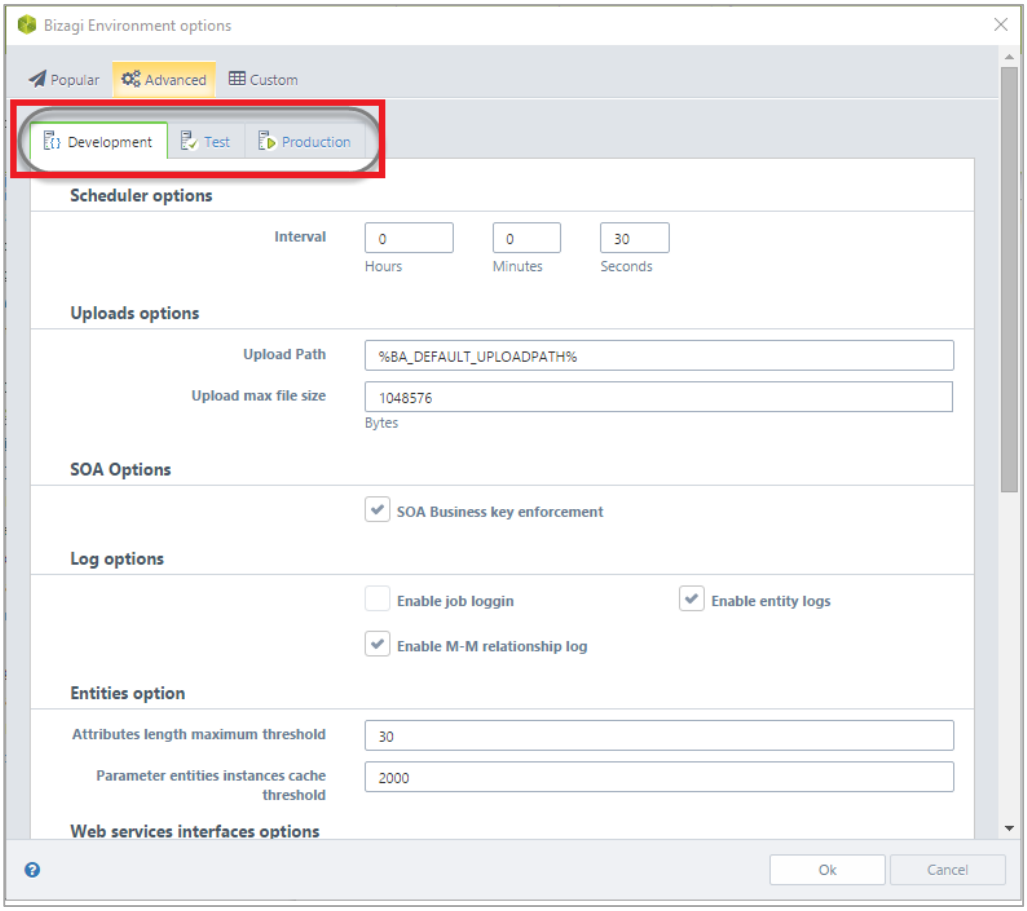
OPCIÓN	DESCRIPCIÓN
Configuración de correo electrónico	
Habilitar Email	Habilita o deshabilita el envío de correos automáticos. Si se habilita, se enviarán correos electrónicos. De lo contrario, los correos electrónicos se ignorarán.
Servidor SMTP	Define el nombre del servidor SMTP. El SMTP puede ser local (local host) para propósitos de prueba en el ambiente de desarrollo. Para los ambientes de pruebas y producción el servidor debe ser el servidor de la compañía desde donde se envían los correos electrónicos.
Cuenta SMTP	Define la cuenta SMTP (o dirección) utilizada para el envío de correos electrónicos. Debe ser una dirección de correo válida en el servidor SMTP. Si se utiliza un servidor local (local host) la dirección de correo electrónico puede ser una que no válida. Si se utiliza el servidor SMTP real, las direcciones deben pertenecer al dominio.
Enviar copia a	Define una cuenta de correo electrónico a la cual se enviarán las copias de todos los correos enviados por la aplicación.
Enviar copia Oculta a	Define una cuenta de correo electrónico a la cual será enviada una copia OCULTA de todos los correos enviados por la aplicación.
Integración de correo electrónico	
Habilitar revisión de emails	Habilita la posibilidad de recuperar correos electrónicos desde una cuenta configurada para poder completar tareas a través de correo electrónico sin ingresar al Portal de Trabajo.
Tipo de conexión	Depende de los requerimientos de su compañía, las opciones disponibles son *Exchange*, *POP3* e *IMAP*.

Activar SSL	Define si Bizagi usará *SSL* para conectarse con su servidor de correo (recomendado). Esta opción depende de la configuración de su Servidor de Correos y está disponible cuando el tipo de conexión es *POP3* o *IMAP*. Nótese que las conexiones para *Exchange* ya de por si refuerzan el uso obligatorio de *HTTPS*.
Puerto	Define el Puerto de conexión a su Servidor de Correos. Esta opción está disponible cuando el tipo de conexión es *POP3* o *IMAP*.
Cuenta	Define la cuenta que recibirá las respuestas de los correos electrónicos enviados por los usuarios finales.
Servicio de Correo / Servidor	Cuando se selecciona Exchange el campo Servidor debe ser la URL de su directorio virtual EWS. En otras palabras, el servicio de correo recibe la URL del Servicio Web de Exchange, el cual es una ULR .asmx, la URL por defecto para este servicio es https://[MailServer]/EWS/Exchange.asmx. Dé clic aquí para más información sobre Servicio Web de *Exchange* (EWS) y cómo determinarla. Cuando se selecciona *POP3* o *IMAP*, define el nombre o la dirección IP de su Servidor de Correos.
Usuario	Define un nombre de usuario válido dentro de su Servidor de Correos
Clave	La contraseña del usuario previamente mencionado.
Seguridad Web Service	
Habilitar servicios web legados (asmx)	Esta opción da acceso a los servicios legados de Bizagi (asmx). Para más información, consulte Seguridad de servicios web Bizagi.
Habilitar WS-Security	Esta opción da acceso a los servicios seguros de Bizagi (svc). Para más información, consulte Seguridad de servicios web Bizagi.
Usuario	El nombre de usuario usado para firmar. Para propósitos de autenticación de los servicios web, usted debe definir un usuario (como es especificado por el estándar de WS-Security).
Contraseña	Contraseña del usuario mencionado anteriormente.
X509 Valor de búsqueda	El *Common name* del certificado X.509 instalado.
X509 Localización repositorio	La ubicación del repositorio donde el certificado X.509 está instalado. Puede usar el MMC snap-in para verificar dicha información (https://msdn.microsoft.com/en-us/library/ms788967(v=vs.110).aspx).
X509 Nombre repositorio	El nombre del repositorio donde el certificado X.509 está instalado. Usted puede usar el MMC snap-in para verificar dicha información (https://msdn.microsoft.com/en-us/library/ms788967(v=vs.110).aspx).
X509 Tipo de búsqueda	El valor por el cual se filtrará el parámetro *Valor de búsqueda*. Para buscar el *common name* del certificado, use *FindBySubjectName*.
X509 Modo validación	Eliga una de las opciones válidas: •*ChainTrust*: Con esta opción se valida el certificado usando la autoridad certificadora. En escenarios .NET, puede ser más confiable usar esta opción. •*PeerTrust*: Con esta opción se valida con el servidor su repositorio de confianza (recomendado). PeerTrust implica que el certificado entrante debe estar en la carpeta "*Trusted People certificate*". •*None*: Confiar en cualquier certificado (no recomendado).

Fuente: http://help.bizagi.com/bpm-suite/es/index.html?define_the_structure_of_your_p.htm

4.2. Avanzado

Aquí se puede configurar los parámetros de características avanzadas, para los ambientes (desarrollo, pruebas, producción).



Los parámetros para configurar son:

OPCIÓN	DESCRIPCIÓN
Opciones del Scheduler	
Intervalo	Configura el intervalo (en horas, minutos y segundos), para cuan frecuente el servicio de Scheduler monitoreará para ver si hay trabajos pendientes.
Opciones de Upload	
Directorio de Upload	Define el directorio físico en donde se almacenan los archivos cargados por los usuarios. El directorio por defecto en Bizagi es *C:\Bizagi\[Project name]\Docs*.
Tamaño máximo	Define el tamaño máximo que puede tener un archivo para ser subido a la aplicación Bizagi (bytes).

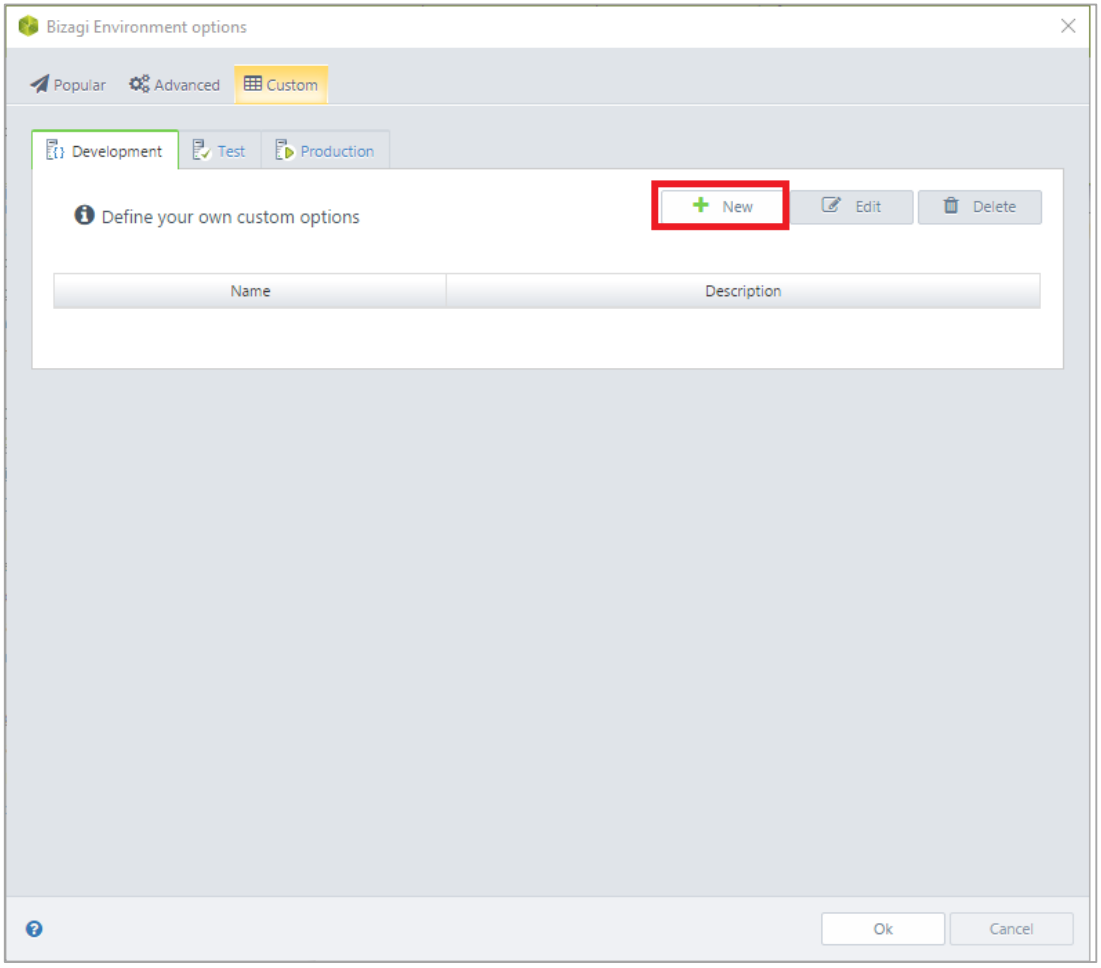
Opciones de SOA	
Forzar llave de negocio de SOA	La opción de deshabilitar esta configuración, aplica para las edición Bizagi .NET. Si está marcado, Bizagi mostrará una excepción para la actualización de registros por medio de la Capa SOA cuando se intente registrar una llave de negocio apuntando a una entidad paramétrica o maestra, cuyo valor no exista en Bizagi. Si no está marcado el valor que no exista quedará en nulo.
Opciones de registro	
Habilitar registro de Jobs	Permite el registro de la información en todos los trabajos en ejecución.
Habilitar registro Entidades	Permite el registro de información en las entidades.
Habilitar registro de relaciones M-M	Si está habilitado, Bizagi crea un registro en la base de datos (Attriblog) con cualquier cambio (relacionar o des-relacionar) relaciones M-M (múltiple-a-múltiple)
Opciones de la Entidad	
(1) Límite máximo de longitud de Atributo Y (2) Límite de instancias de Entidades	Las Entidades Paramétricas en el Portal de Trabajo se manejan en caché si la longitud de los atributos es menor que el primer parámetro y el número de registros es menor que el segundo parámetro.
Opciones de Interfaces de Servicios Web	
Tiempo de Espera	Sirve para configurar un TimeOut para los WebServices sincrónicos. Si el valor especificado es menor o igual a cero, se ignorará, comportándose por defecto: el llamado espera una respuesta con éxito o con error, sin importar el tiempo que tome. Dado que esto puede generar bloqueos y se sugiere configurar un valor.
Umbral para registro	Tiempo del umbral en segundos para el log de interfaces que duran más de este tiempo.
Opciones de notificaciones de anulación	
Deshabilitar notificaciones de anulación	Si se selecciona desactiva la notificación de los casos que sean anulados. Estas notificaciones se envían a todas las personas que tengan tareas pendientes en el caso en cuestión.
Almacén de datos operativos	
Proveedor	Configuración del uso de la conexión ODS para el proyecto. Para más información diríjase a Configuración ODS
ODS del motor de consultas	
Proveedor	Configuración del uso de la conexión ODS para el motor de consultas. Para más información diríjase a Habilitar soporte a query engine
Seguridad	

Dominios confiables (CORS) *Cross-origin Resource Sharing*	Defina los dominios que pueden interactuar con Bizagi. Si ningún dominio se define, por defecto todos los dominios son habilitados. Los dominios deben estar separados por comas.

4.3. Personalizado

Aquí se puede agregar, editar y borrar los diferentes parámetros del proyecto para los ambientes (desarrollo, pruebas, producción).

a) Para crear nuevos parámetros, dé clic en el botón. En esta nueva ventana, defina el nombre, valor y descripción del parámetro.



b) Para editar algún parámetro creado, dé clic en Editar y cambios los campos que desee.

c) Para elimina un parámetro, dé clic en Eliminar y eliminará el parámetro.

ANEXO 2

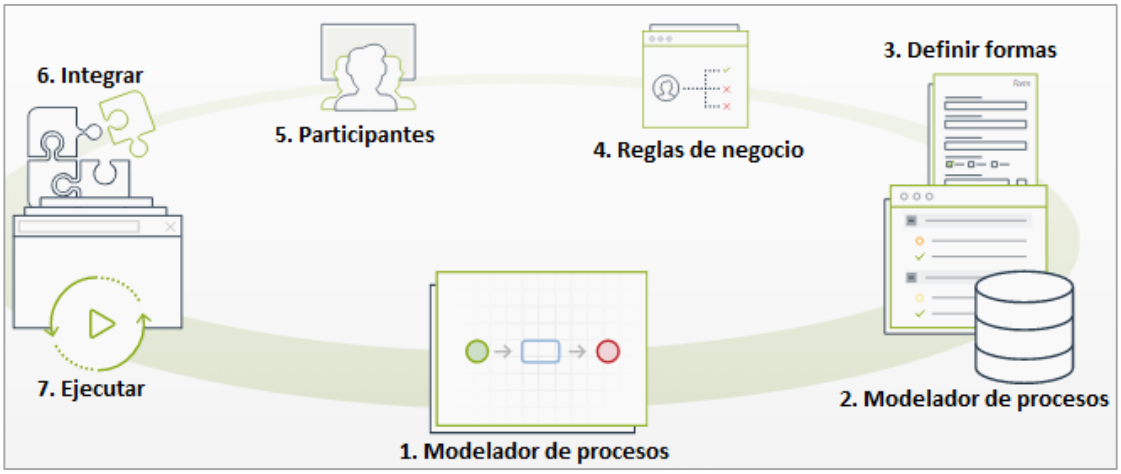
MANUAL DE USUARIO

Contenido

1. Asistente de procesos de Bizagi
2. Simbología de Bizagi
3. Sistema

1. Asistente de procesos

Bizagi provee 7 pasos necesarios para automatizar los procesos.



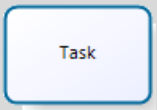
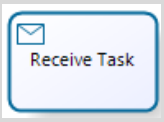
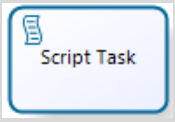
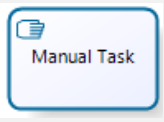
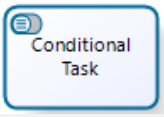
- **Modelar Procesos**: Aquí se define el flujo del proceso.
- **Modelar Datos**: Aquí se diseña un modelo de datos.
- **Definir Formas**: Aquí se diseña las interfaces de usuario y la información que será mostrada en las actividades del proceso.
- **Reglas de Negocio**: Aquí se define las condiciones de flujo y se realizan las expresiones para definir el comportamiento.
- **Participantes**: Aquí se asigna los usuarios que serán responsables de los procesos.
- **Integrar:** Aquí se configura las conexiones con los sistemas externos o entre procesos. Este paso es opcional.
- **Ejecutar**: Lleve sus procesos a ambientes de pruebas y de producción.

2. Simbología de Bizagi

Las actividades son las tareas que realizan los miembros de la organización, éstas se pueden ejecutar manual o automáticamente. Las actividades se clasifican en tareas y subprocesos.

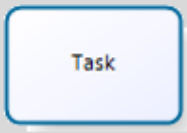
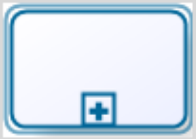
2.1. Tareas

Las tareas son actividades atómicas utilizadas cuando el trabajo que se está realizando no se puede descomponer a un nivel más detallado.

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Tarea	Es una actividad atómica dentro de un flujo de proceso. Se utiliza cuando el trabajo en proceso no puede ser desglosado a un nivel más bajo de detalle.	
Tarea de Servicio	Es una tarea que utiliza algún tipo de servicio que puede ser Web o una aplicación automatizada.	
Tarea de Recepción	Es una tarea diseñada para esperar la llegada de un mensaje por parte de un participante externo (relativo al proceso).	
Tarea de Envío	Es una tarea diseñada para enviar un mensaje a un participante externo (relativo al proceso).	
Tarea de Script	Es una tarea que se ejecuta por un motor de procesos de negocio. El usuario define un script en un lenguaje que el motor pueda interpretar.	
Tarea Manual	Es una tarea que espera ser ejecutada sin la asistencia de algún motor de ejecución de procesos de negocio o aplicación.	
Tarea Condicional	Es una tarea diseñada para que se lance cuando se cumpla una cierta condición.	

2.2.Subprocesos

Un subproceso es una actividad compuesta que se incluye dentro de un proceso.

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Subproceso Embebido	Es una actividad cuyos detalles internos han sido modelados utilizando actividades, compuertas, eventos y flujos de secuencia. La forma tiene una borde delgado.	
Subproceso Reusable	Identifica un punto en el flujo donde se invoca un proceso pre-definido. Los procesos reutilizables se conocen como Actividades de Llamada en BPMN. La forma tiene un borde grueso.	
Subproceso transaccional	Es un Subproceso cuyo comportamiento es controlado a través de un protocolo de transacción. Este incluye los tres resultados básicos de una transacción: Terminación exitosa, terminación fallida y evento intermedio de cancelación.	
Subproceso múltiple	Los Subprocesos pueden repetirse secuencialmente comportándose como un ciclo. El ciclo multi-instancia permite la creación de un número deseado de instancias de actividad que pueden ser ejecutadas de forma paralela o secuencial.	

2.3. Compuertas

Las compuertas se utilizan para controlar la divergencia y convergencia de flujos de secuencia. Determinan ramificaciones, bifurcaciones, combinaciones y uniones en el proceso.

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Compuerta Exclusiva	De divergencia: Se utiliza para crear caminos alternativos dentro del proceso, pero solo uno se selecciona. De convergencia: Se utiliza para unir caminos alternativos.	
Compuerta Basada en Eventos	Representa un punto de ramificación en los procesos donde los caminos alternativos que siguen la compuerta están basados en eventos que ocurren. Cuando el primer evento se dispara, se usará el camino que sigue a ese evento. Los caminos restantes serán deshabilitados.	
Compuerta Paralela	De divergencia: Se utiliza para crear caminos alternativos sin evaluar condición alguna. De convergencia: Se utiliza para unir caminos alternativos. Las compuertas esperan todos los flujos que concurren en ellas antes de continuar.	
Compuerta Compleja	De divergencia: Se utiliza para controlar puntos de decisión complejos en los procesos. Crea caminos alternativos dentro del proceso utilizando expresiones. De convergencia: Permite continuar al siguiente punto del proceso cuando una condición de negocio se cumple.	
Compuerta Inclusiva	De divergencia: Representa un punto de ramificación en donde las alternativas se basan en expresiones condicionales. La evaluación VERDADERA de una condición no excluye la evaluación de las demás condiciones. Todas las evaluaciones VERDADERAS serán atravesadas por un token. De convergencia: Se utiliza para unir una combinación de caminos paralelos alternativos.	

2.4. Eventos

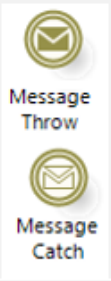
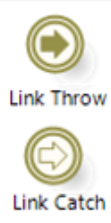
Un evento es algo que sucede durante el curso del proceso, afectando el flujo y generando un resultado.

- **Eventos de Inicio**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Evento de Inicio Simple	Indica dónde se inicia un proceso. No tiene algún comportamiento particular.	
Evento de Inicio de Mensaje	Se utiliza cuando el inicio de un proceso se da al recibir un mensaje de un participante externo.	

Evento de Inicio de Temporización	Se utiliza cuando el inicio de un proceso ocurre en una fecha o tiempo de ciclo específico. (e.g, todos los viernes)	
Evento de Inicio de Señal	El inicio de un proceso se da por la llegada de una señal que ha sido emitida por otro proceso. Tenga en cuenta que la señal no es un mensaje; los mensajes tienen objetivos específicos, la señal no.	

- **Eventos Intermedios**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Evento Intermedio Simple	Indica que algo sucede en algún lugar entre el inicio y el final de un proceso. Esto afectará el flujo del proceso, pero no iniciará (directamente) o finalizará el mismo.	
Evento de Mensaje	Indica que un mensaje puede ser enviado o recibido. Si un proceso está esperando un mensaje y éste es capturado, el proceso continuará su flujo. El marcador de eventos en esta instancia estará lleno. El evento que lanza un mensaje se identifica con una figura sombreada. El evento que capta un mensaje se identifica con una figura sin relleno.	
Evento de Temporización	Indica un retraso dentro del proceso. Este tipo de evento puede ser utilizado dentro de un flujo secuencial para indicar un tiempo de espera entre actividades.	
Evento de Enlace	Este evento se utiliza para conectar dos secciones del proceso. Los eventos de enlace pueden ser utilizados para crear ciclos o evitar líneas de secuencia de flujo largas.	
Evento de Señal	Estos eventos se utilizan para enviar o recibir señales dentro o a lo largo del proceso. Una señal es similar a una bengala que se dispara al cielo para cualquiera que pueda estar interesado en ella y reaccionar.	
Evento condicional	Es un evento diseñado para que se lance cuando se cumpla una cierta condición.	

- **Eventos Intermedios adjuntos a los límites de una Actividad**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Evento Temporizador	Si un Evento Temporizador se encuentra adjunto a los límites de una actividad, cambiará el flujo normal a un flujo de excepción cuando se cumpla un ciclo determinado o se alcance una fecha específica. Si interrumpe la actividad a la que se encuentra adjunto, los bordes de la figura se mostrarán sólidos, de lo contrario se mostrarán discontinuos.	
Evento de Error	Un Evento Intermedio de Error solo puede ser adjunto a los límites de una actividad. Este evento captura un error específico (si se le asigna un nombre) o cualquier error (si no se especifica nombre). El Evento de Error siempre interrumpe la actividad a la cual se encuentra adjunto, por lo que no existe una versión "No interruptor" de éste y en consecuencia, los bordes de la figura se muestran siempre sólidos.	
Evento de Cancelación	Este evento es utilizado en Subprocesos transaccionales y debe ir adjunto a los límites de uno. El evento se dispara si se alcanza un Evento de fin de Cancelación dentro del Subproceso de transacción o, si se recibe un mensaje de cancelación de un protocolo de cancelación mientras la transacción se encuentra en ejecución. El Evento de Cancelación siempre interrumpe el Subproceso al cual se encuentra adjunto, por lo que no existe una versión "No interruptor" de éste y en consecuencia, los bordes de la figura se muestran siempre sólidos.	
Evento de Compensación	Cuando se encuentra adjunto a los límites de una actividad, este evento se utiliza para capturar la compensación. Cuando esto ocurre, la actividad de compensación será ejecutada. La interrupción o no interrupción de la actividad no aplica para el Evento de Compensación, por lo que los bordes de la figura siempre se mostrarán sólidos.	

- **Eventos de Finalización**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Finalización simple	Indica que el flujo finaliza.	
Finalización de Mensaje	Indica que se envía un mensaje una vez finaliza el flujo.	
Finalización de Error	Indica que se debe generar un error. Todas las secuencias activas del proceso son finalizadas. El error será recibido por un evento intermedio de captura de error.	
Finalización de Cancelación	Se utiliza dentro de un Subproceso de transacción e indica que éste debe ser cancelado.	
Finalización de Señal	Indica que una señal es enviada una vez finaliza el flujo.	
Finalización Terminal	Finaliza el proceso y todas sus actividades de forma inmediata.	

- **Artefactos**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Grupo	Es un artefacto que provee un mecanismo visual para agrupar elementos de un diagrama de manera informal.	
Anotación	Son mecanismos para que un modelador provea información adicional, al lector de un diagrama.	
Objetos de datos	Proveen información sobre cómo documentos, datos y otros objetos son utilizados y actualizados durante el proceso.	

- **Carriles (Swim lanes)**

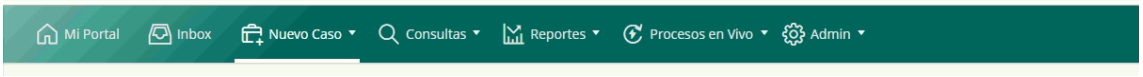
ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Contenedor (Pool)	Un pool es un contenedor de procesos simples (contiene flujos de secuencia dentro de las actividades). Un proceso está completamente contenido dentro de un pool. Siempre existirá al menos un pool.	
Carril (Lane)	Es una sub-partición dentro del proceso. Los lanes se utilizan para diferenciar roles internos, posiciones, departamentos, etc.	
Fase	Es una sub-partición dentro del proceso. Puede indicar diferentes etapas durante el mismo.	

- **Conectores**

ELEMENTO	DESCRIPCIÓN	NOTACIÓN
Flujo de Secuencia	Un flujo de secuencia es utilizado para mostrar el orden en el que las actividades se ejecutarán dentro del proceso.	
Asociación	Se utiliza para asociar información y artefactos con objetos de flujo. También se utiliza para mostrar las tareas que compensan una actividad.	
Flujo de Mensaje	Se utiliza para mostrar el flujo de mensajes entre dos entidades que están preparadas para enviarlos y recibirlos.	

3. Portal de trabajo

El portal de trabajo presenta el siguiente menú:



Descripción del menú principal:

- Mi Portal

OPCIÓN	DESCRIPCIÓN
Mi Portal	Muestra las cosas, planes y casos del usuario de acuerdo con la experiencia diseñada para el Stakeholder en Bizagi Studio.

- Inbox

OPCIÓN	DESCRIPCIÓN
Inbox	Muestra las actividades pendientes del usuario y el estado de cada una. Los diferentes estados (a tiempo, en riesgo y expirado) se representan con diferentes colores para una fácil identificación.

- Nuevo

OPCIÓN	DESCRIPCIÓN
Crear	Crea un nuevo caso o instancia de proceso, del proceso seleccionado. Los procesos se muestran de acuerdo con la estructura del proyecto: Aplicación, Categoría, Subcategoría y Proceso.

- Consultas

OPCIÓN	DESCRIPCIÓN
Consultas	Permite acceder a la data de los casos por medio de consultas personalizadas. Estas consultas se usan para lleva a cabo búsquedas que cumplan con ciertos criterios de negocio o de proceso. Estos reportes permiten realizar análisis gráfico.

- Reportes, este menú da acceso a los informes de rendimiento de los procesos.

OPCIÓN	SUB-OPTION	DESCRIPCIÓN
BAM	Procesos	El BAM de procesos le permite analizar el estado de casos activos.
	Tareas	El BAM de tareas le permite analizar el estado de actividades pendientes.
	Monitor de recursos	El Monitor de Recursos le permite analizar la carga y desempeño de usuarios y grupos de trabajo.
Análisis	Procesos	El Análisis de Procesos presenta un resumen de casos y actividades cerrados.
	Tareas	El Análisis de Tareas presenta información de Actividades que pertenecen a casos cerrados.
Sensores	Sensores	Los Sensores le proporcionan información de los caminos y contadores definidos por el usuario.
Mis Reportes	Mis Reportes	Mis reportes dan acceso a los reportes guardados por usted.

- Procesos en Vivo
  Este menú le permite crear proceso directamente desde el portal de trabajo.

- Admin

OPCIÓN	DESCRIPCIÓN
Administrar Procesos en Vido	Permite administrar los procesos en vivo creados por los usuarios para publicarlos o administrarlos bajos sus diferentes estados.
Nuevo Proceso en Vivo	Permite producir un nuevo Proceso en Vivo.

Las siguientes opciones deben ser manejadas por un administrador.

OPCIÓN	DESCRIPCIÓN
Entidades	Permite la administración de Entidades Paramétricas para modificar, añadir o deshabilitar registros.
Usuarios	Permite la administración de los usuarios: creación o actualización.

OPCIÓN	DESCRIPCIÓN
Políticas del negocio	Administra las Políticas de negocio, Grupos de políticas, precondiciones, Tablas de decisión y Vocabularios, en tiempo real.
Constructor de Temas	Abre en una nueva ventana el constructor de temas, permitiendo al usuario modificar el diseño del portal de trabajo, el ícono y personalizar cada componente del portal de trabajo.
Stakeholders	Permite la administración de los usuarios asociados a Stakeholders.
Búsqueda en el registro de autenticación	Permite revisar el log de las autenticaciones hechas por usuarios.
Cifrado de clave	Cifra las contraseñas usadas en la base datos para incrementar la seguridad del acceso a la información.
Solicitudes pendientes de usuarios	Despliega las solicitudes pendientes de las cuentas de usuarios bloqueadas.
Casos	Permite reasignar las Actividades o abortar casos.
Consola de actividades asíncronas	Maneja las actividades asíncronas que han fallado.
Administrar asignación de usuario predeterminado	Permite la definición o modificación de los usuarios para la asignación predeterminada de los procesos. Recuerde que un usuario predeterminado se utiliza para asignar los casos en que los criterios de asignación no se cumplen.
Perfiles	Permite la inclusión o borrado de los usuarios de: Posiciones, roles, habilidades, grupos de usuario y Organización.
Alarmas	Permite generar alertas o alarmas cuando una actividad va a expirar o ha expirado.
Licencias	Permite la administración de Licencias.
Dimensiones	Permite al usuario crear, editar y eliminar Dimensiones

- Buscar

OPCIÓN	DESCRIPCIÓN
Buscar	Permite buscar casos por su número de creación, y datos a través de las búsquedas predefinidas.

4. Sistema

4.1. Opciones de inicio de sesión

Para iniciar sesión, ingrese su usuario, contraseña y dominio.

- **Recordar mi usuario y contraseña**: Si se selecciona esta opción, la próxima vez que acceda al Portal de Trabajo, ingresará automáticamente.

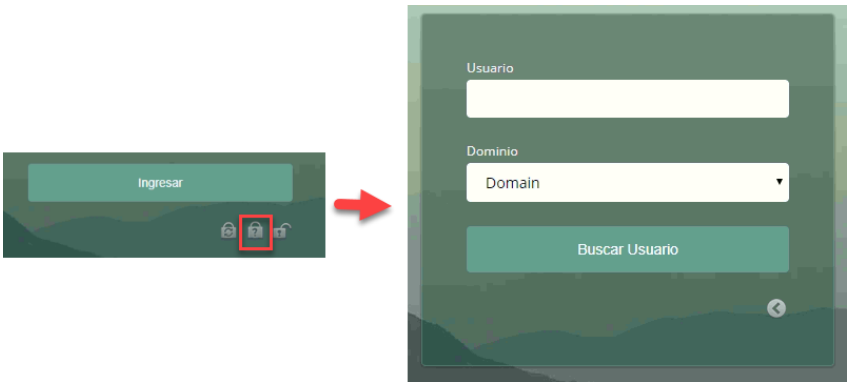
- **Recordar mi cuenta**: Si se selecciona esta opción, la próxima vez que acceda al Portal de Trabajo, se mostrará su usuario (y dominio) automáticamente diligenciado.
- **Preguntar siempre por cuenta y contraseña:** Por defecto o cuando se seleccione esta opción, nada cambiará con respecto al primer inicio de sesión.
-

4.2. Opciones de cuenta

- **Cambiar contraseña**

  Se le solicitará: usuario, dominio, la contraseña actual y la nueva contraseña junto con su confirmación.

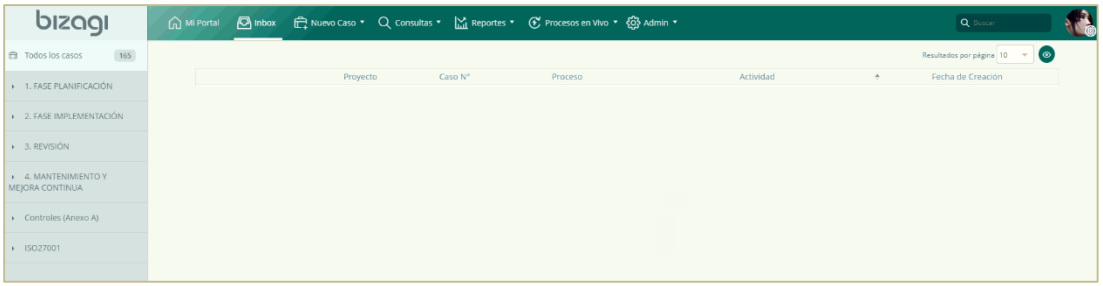
- **Olvidó su contraseña**
  Le permite reiniciar la contraseña de su cuenta, si, por ejemplo, la ha olvidado. La nueva contraseña será enviada a través de correo electrónico después de este procedimiento.



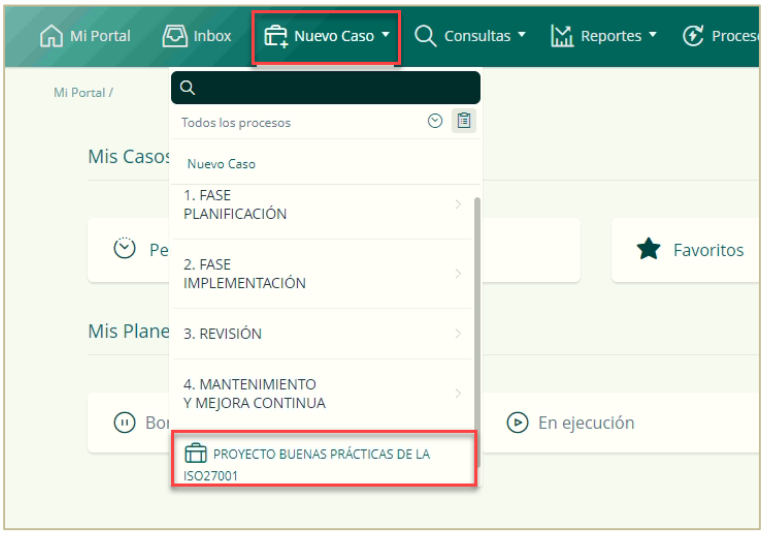
- **Desbloquear cuenta**
  Le permite enviar una solicitud a su administrador por medio de correo electrónico, para que su cuenta pueda ser desbloqueada. El bloqueo de una cuenta puede suceder por varias razones, incluyendo que se alcance el número máximo de inicios fallidos de sesión.

4.3. Crear casos

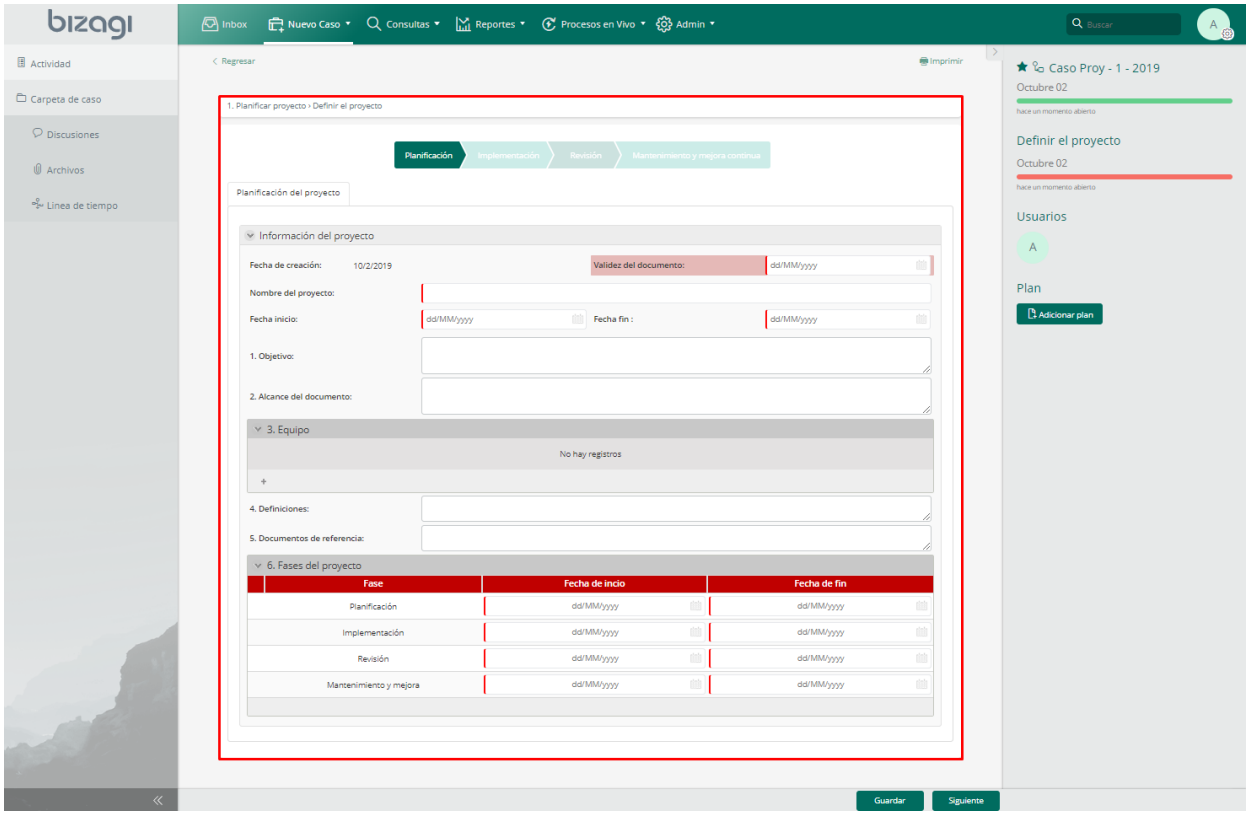
- A continuación, mostramos la pantalla principal.



a) Para crear un caso, dé clic en **Nuevo caso > PROYECTO BUENAS PRÁCTICAS DE LA ISO 27001**.

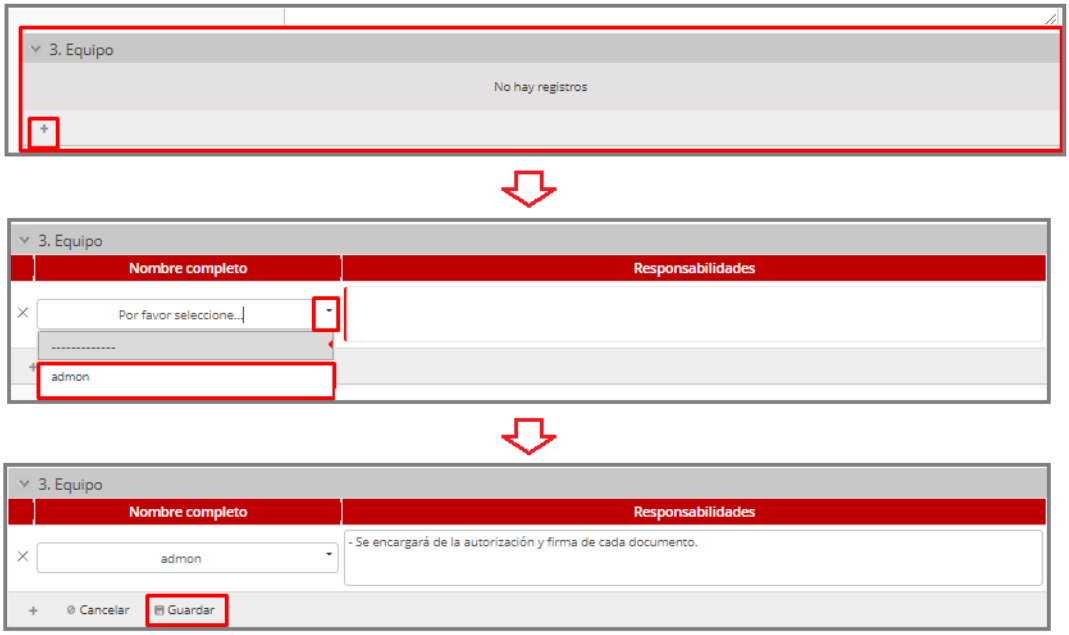


b) Se mostrará el siguiente formulario, ingresamos la información correspondiente de cada campo. Por defecto, se muestra la fecha actual en el campo fecha de creación.

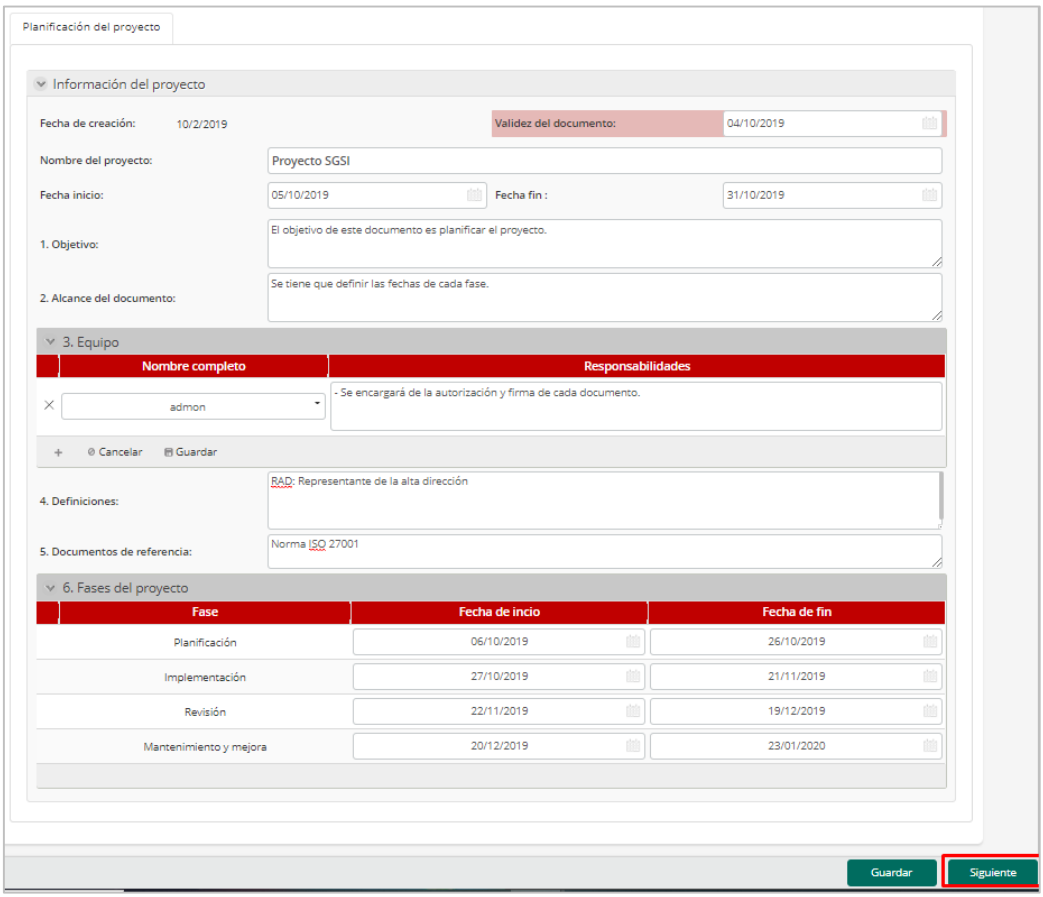


Los campos que tienen una línea roja a la izquierda indican que son obligatorios.

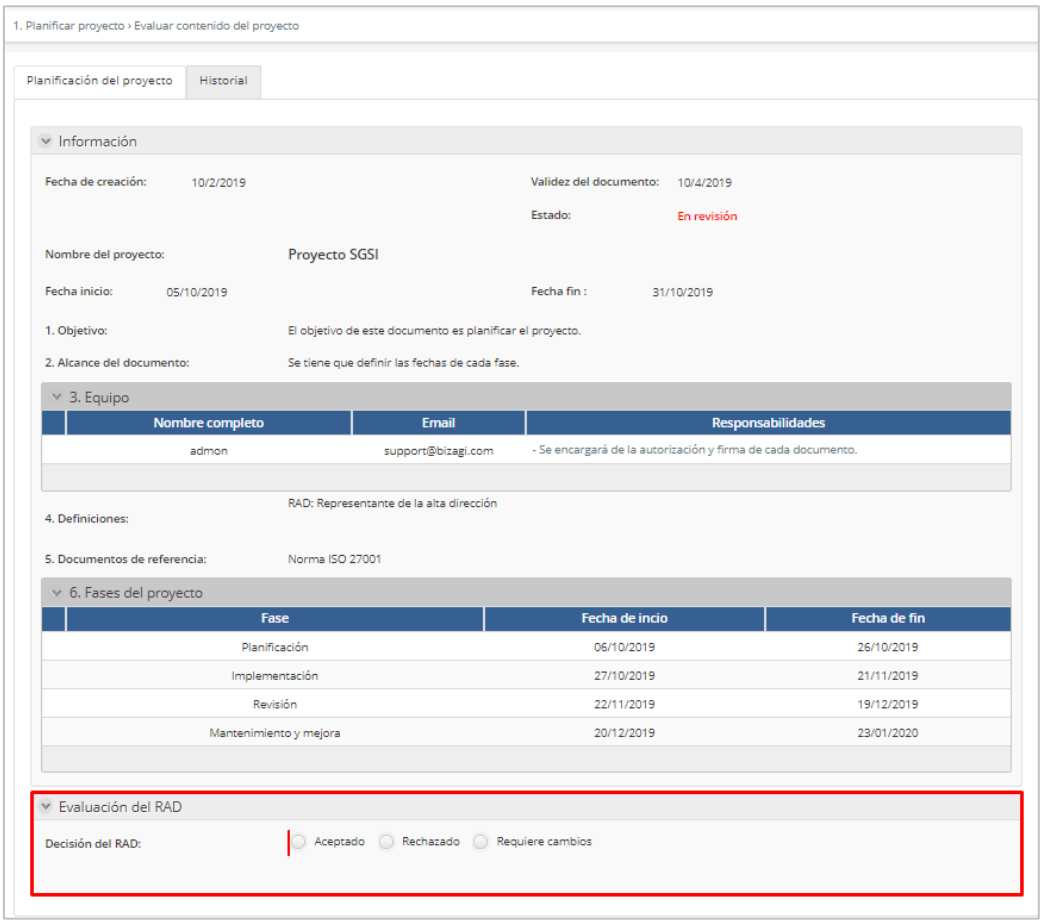
c) Para agregar miembros al equipo, dé clic en +, y mostrará una nueva fila. Se listará todos los usuarios que existe en el sistema.

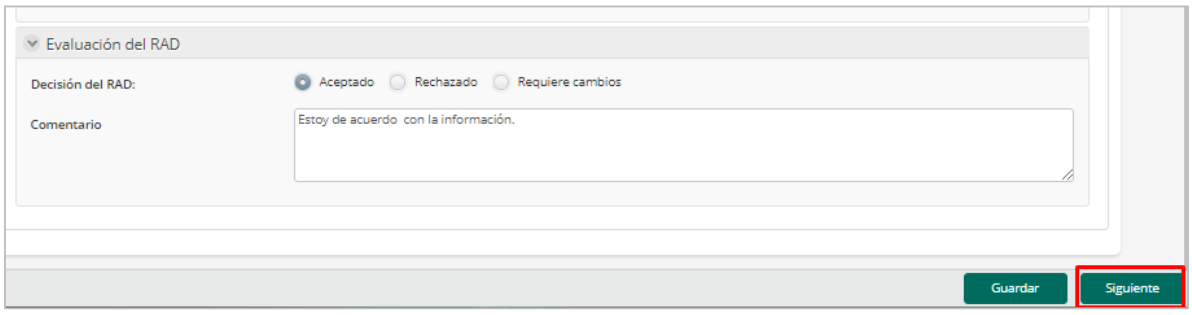


d) Una vez ingresada toda la información, dé clic en siguiente.

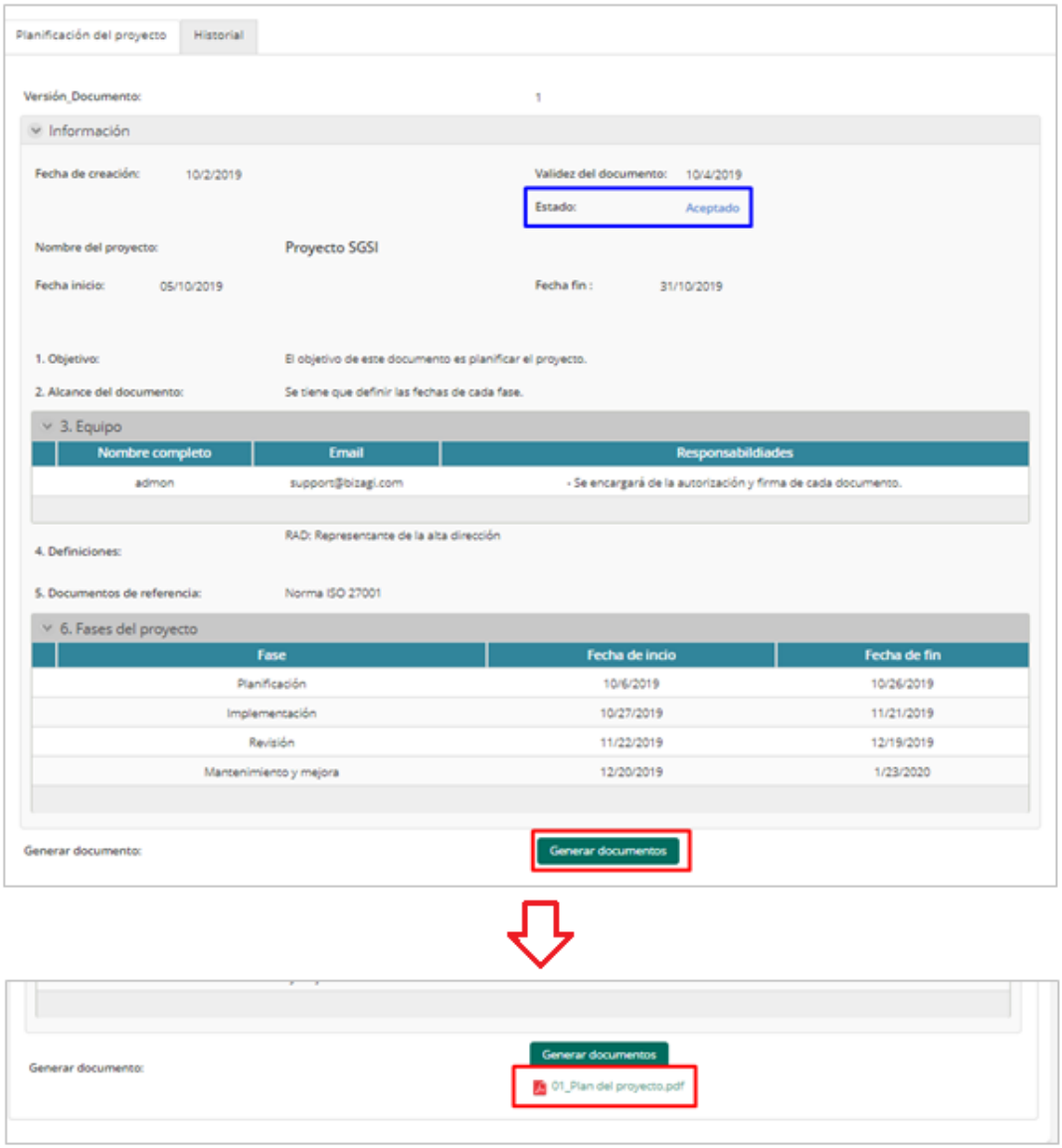


e) El siguiente paso es la evaluación del RAD, mostrará el formulario con todos los datos ingresados por el jefe de seguridad. En la parte inferior del formulario, el RAD tendrá que dar su evaluación.





f) Una vez ingresada el comentario, dé clic en siguiente.
En este paso, el jefe de seguridad tiene que generar e imprimir el documento para que el RAD lo firme. Clic en Generar documento, se generará el documento en PDF > clic en siguiente.



g) Vista preliminar del documento generado.

PLAN DEL PROYECTO PARA LA IMPLEMENTACIÓN DE LAS BUENAS PRÁCTICAS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código	Plan-01
Versión:	1.0
Fecha de la versión:	02/10/2019
Creado por:	Admin
Aprobado por:	Admin
Nivel de confidencialidad:	Uso interno
Estado:	Aprobado

HISTORIAL DE MODIFICACIONES

Fecha	Etapa	Versión	Responsable	Descripción
02/10/2019 0:48:36	Creada	1.0	admon	Proyecto SGSI
02/10/2019 0:54:09	Revisada	1.0	admon	Estoy de acuerdo con la información.

1. OBJETIVO

El objetivo de este documento es planificar el proyecto.

2. ALCANCE

Se tiene que definir las fechas de cada fase.

3. RESPONSABILIDADES

Nombre completo	email	Reponsabildiades
admon	support@bizagi.com	- Se encargará de la autorización y firma de cada documento.

4. DEFINICIONES

RAD: Representante de la alta dirección

5. DOCUMENTOS DE REFERENCIA

Norma ISO 27001

6. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

Etapa	Fecha de inicio	Fecha final
Planificación	06/10/2019 0:00:00	26/10/2019 0:00:00
Implementación	27/10/2019 0:00:00	21/11/2019 0:00:00
Revisión	22/11/2019 0:00:00	19/12/2019 0:00:00
Mantenimiento y mejora	20/12/2019 0:00:00	23/01/2020 0:00:00

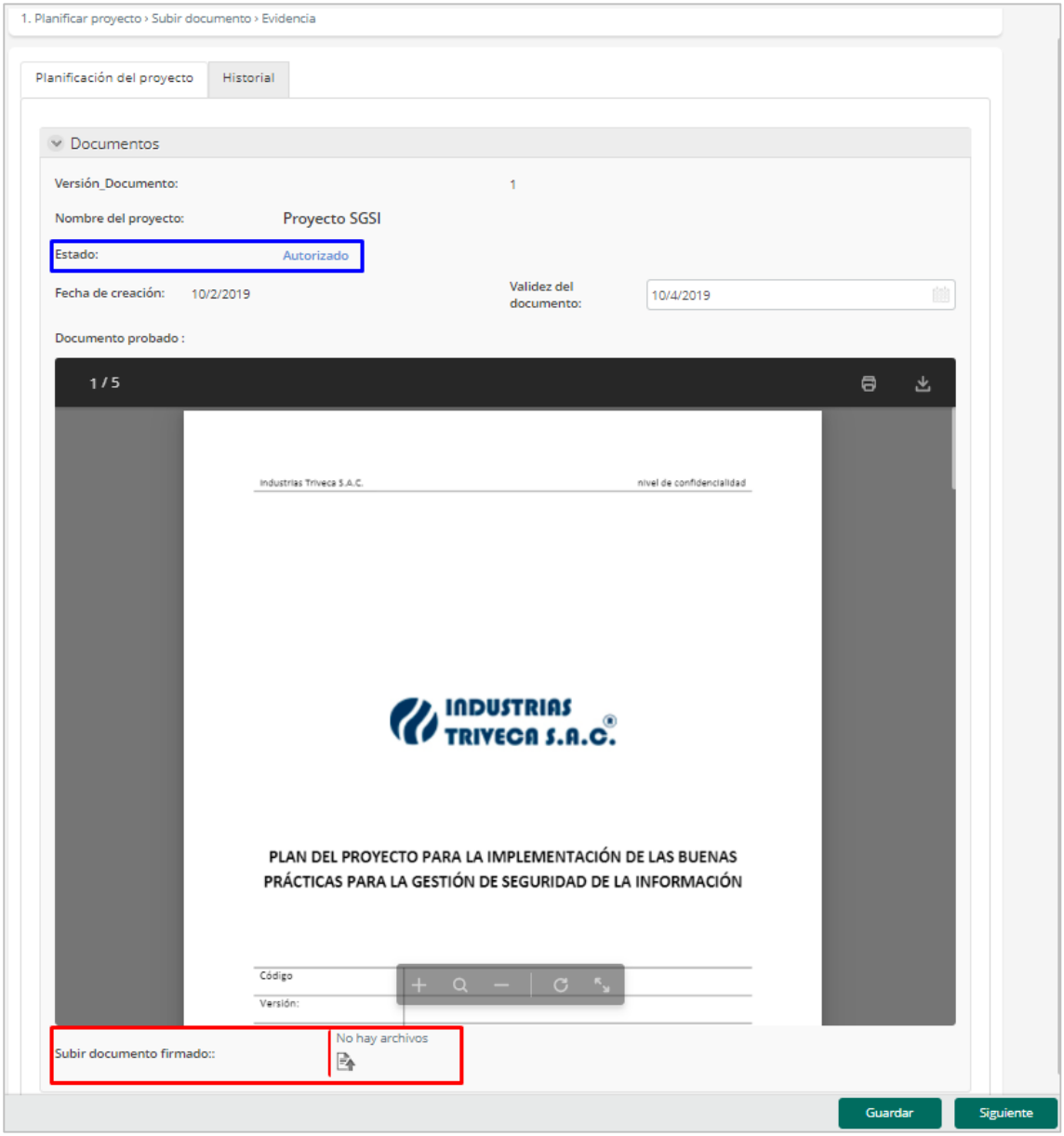
7. Validez

Este documento es válido hasta la fecha 04/10/2019 0:00:00.

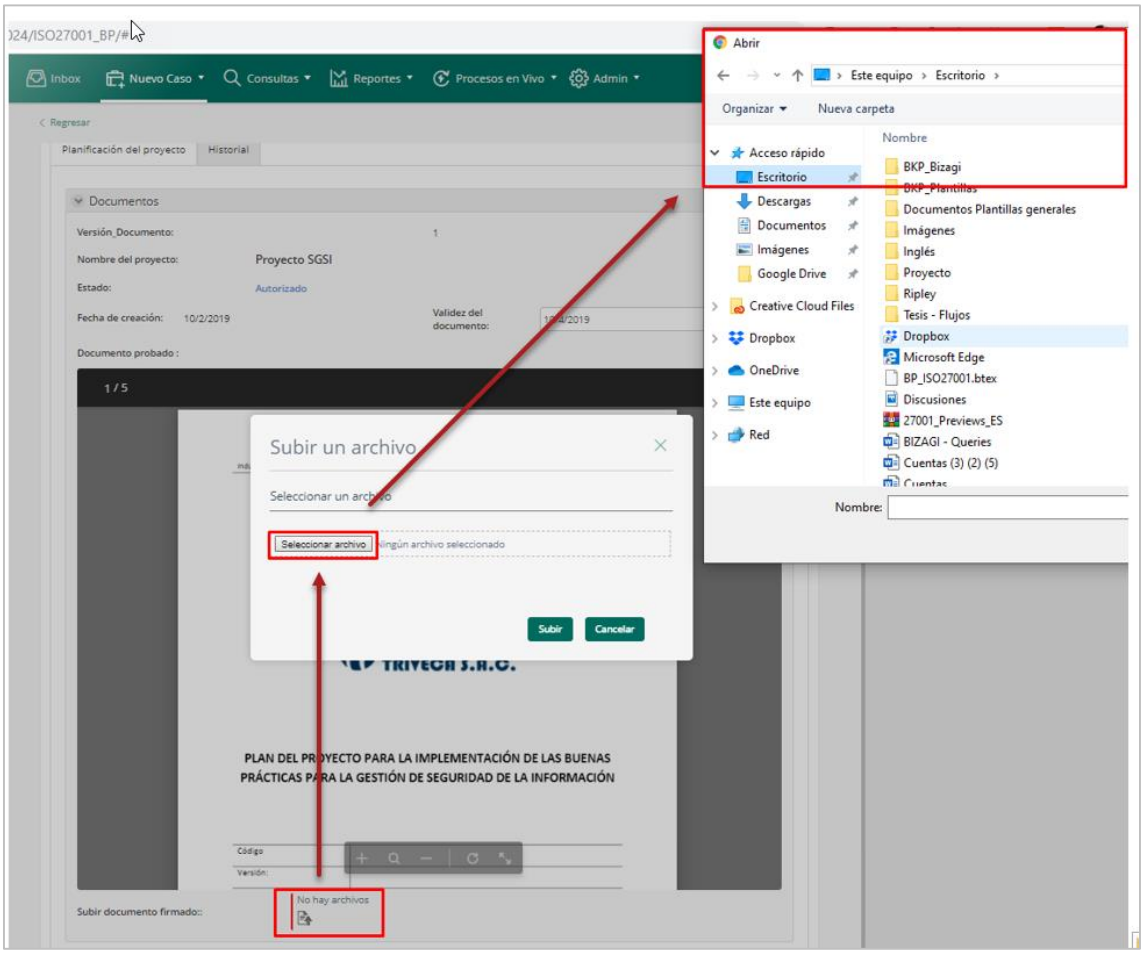
Xiomar Serna

Representante de alta dirección

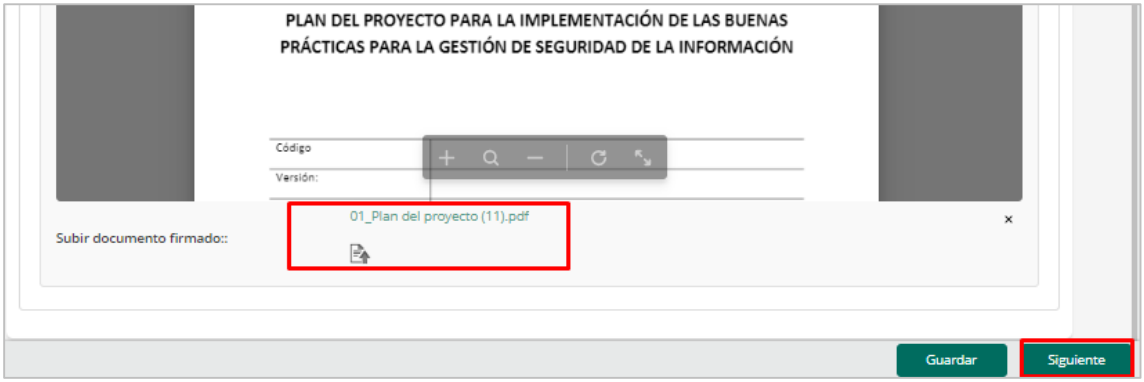
h) El siguiente paso es subir la evidencia, esta nueva ventana muestra el documento aceptado. La evidencia es el documento firmado por el RAD. Clic en Archivo (cuadro rojo)



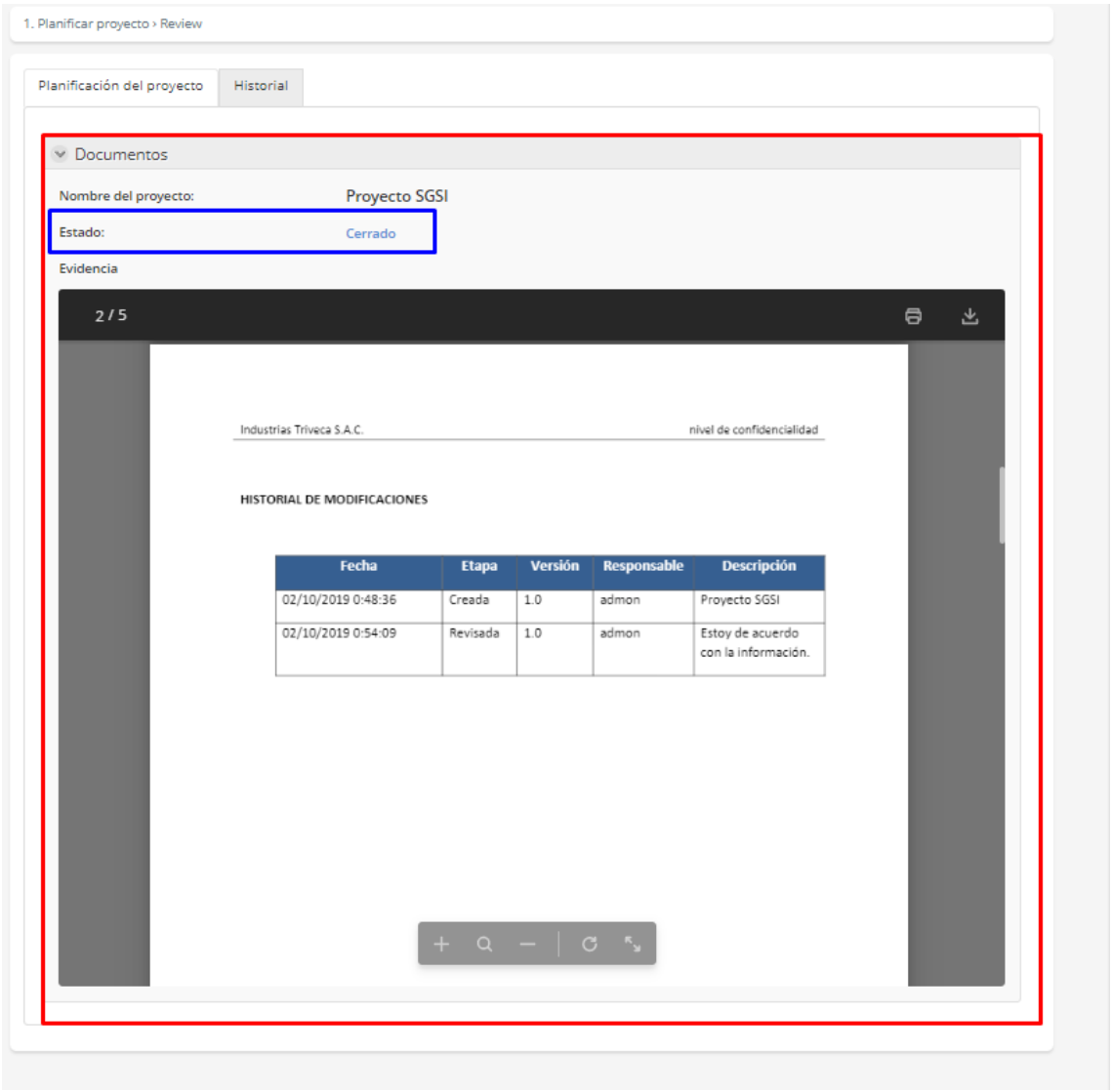
i) Se abrirá una ventana, clic en seleccionar archivo > Se abrirá la carpeta de escritorio. Una vez seleccionado el archivo, dé clic en subir.



i) Una vez subido el documento, de clic en siguiente.



j) Esta última ventana te mostrará un review del proceso con la vista del documento firmado.



k) Para ver todos los casos, de clic en Inbox y mostrará todos los casos.