TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

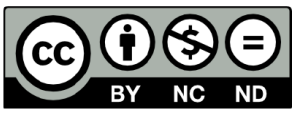
Elaborado por: Sergio Arroyo Torres

Prof. Tutor: Ing. Yarima Sandoval Sánchez, M.A.E

Cartago, Costa Rica

II Semestre

Setiembre, 2022



Hoja de Aprobación

ÁREA ACADÉMICA DE ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

Los miembros de Tribunal Examinador del Área Académica de Administración de Tecnología de Información, recomendamos que el siguiente Trabajo Final de Graduación del estudiante Sergio Jesús Arroyo Torres sea aceptado como requisito parcial para optar por el grado académico de Licenciatura en Administración de Tecnología de Información.

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2022.12.02 16:37:41 -06'00'

Ing. Yarima Sandoval Sánchez

Coordinación Trabajo Final de Graduación

NESTOR ALEJANDRO MORALES RODRIGUEZ (FIRMA)

Firmado digitalmente por NESTOR ALEJANDRO MORALES RODRIGUEZ (FIRMA)
Fecha: 2022.12.01 10:11:02 -06'00'

Lic. Néstor Morales Rodríguez

Lector

LUIS CARLOS NARANJO ZELEDON (FIRMA)

Firmado digitalmente por LUIS CARLOS NARANJO ZELEDON (FIRMA)
Fecha: 2022.12.02 12:22:18 -06'00'

Dr. Luis Naranjo Zeledón

Lector

Nota Aclaratoria

Género[1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del “género inclusivo”. Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del “género inclusivo”. Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

Esparza, 19 de setiembre de 2022

Señores
Área Académica de Admin. de Tecnologías de Información
Instituto Tecnológico de Costa Rica
Cartago, Costa Rica

Por este medio hago constar que he revisado y corregido la sintaxis, la morfología y la semántica del texto: "Propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech" propiedad de Sergio Arroyo Torres, presentado como requisito para optar por el grado académico de Licenciatura en Administración de Tecnología de Información.

Cordialmente,

MAGDALENA VENEGAS PORRAS (FIRMA)
Firmado digitalmente por MAGDALENA VENEGAS PORRAS (FIRMA)
Fecha: 2022.09.19 23:24:53 -06'00'

Lcda. Magdalena Venegas Porras
Filóloga
Carné 10785
Cédula 6-230-116

Dedicatoria

A Cendry Torres, Sergio Arroyo y Carolina Arroyo, por ser mi motivación, mi fuerza y mi vida entera. A ustedes, por todo el apoyo, paciencia y amor invertido durante tantos años; esto es más de ustedes que mío. Aunque sé que tardó más de lo esperado la recompensa es grata; esto no lo habría logrado sin su apoyo. Si hoy entrego esto, es por el amor que les tengo.

A Juan José Varela, mi hermano. Gracias por la compañía, la inspiración y las risas. No sería el mismo sin su apoyo.

A Marco Brenes, por sacarme de la zona de confort y confiar tanto en mi persona. Eternamente agradecido.

A Sussana Ramírez y Leonardo Aguilera, por tantos años de sufrimiento, risas y experiencias. El TEC no hubiera sido lo mismo sin ustedes.

A Dayana Vindas y Néstor Morales, por su atención y ayuda en los momentos más importantes. Y a Dayana, por orientarme y escucharme cuando más lo necesitaba.

A Margarita Ramos y Andrea Alpízar, por darme las herramientas y la confianza necesaria para convertirme en el profesional que soy. Gracias por ver en mí lo que yo no había logrado descubrir de mí mismo.

A mi tutora, Yarima, porque más que un impulso académico fue un impulso emocional en momentos difíciles.

A Alex Ureña y José Méndez, por darme la oportunidad de formar parte de la familia Xumtech y por apoyar todo este proceso.

A Sirleny, Fernanda, Victor, Raquel, Sharon, Lerroy, María José, Lorenzo y Valeria, por ser mis acompañantes durante las distintas etapas de este proceso; por todo el amor, paciencia y atención brindados.

A quienes olvidé pero que formaron parte de esto: ¡Mil gracias!

Resumen

Este documento tiene como objetivo mostrar el análisis realizado, con el fin de seleccionar y proponer políticas de seguridad de la información que promuevan una gestión articulada de los procesos de seguridad en todos los colaboradores de la organización.

Esta investigación está basada en la metodología alternativa, la cual conlleva la demostración de tres dimensiones: epistemológica, ontológica y axiológica. Además, se definieron tres fases que contemplan las actividades necesarias para entender y solucionar la problemática. La primera fase comprende la delimitación de las políticas que formarán parte de la propuesta, así como los procesos que contiene cada una de estas políticas. Además, se incluyen detalles como la diagramación *As-Is* de la situación actual y la explicación y medición de las oportunidades de mejora para cada política. La segunda fase tiene como principal objetivo establecer la brecha entre la situación actual y el marco de referencia COBIT 5, así como la diagramación de los procesos y políticas resultantes del análisis de la brecha. Como última fase, se realiza la simulación de las políticas sobre las cuales se pueda simular, para luego realizar una medición de la efectividad de las políticas propuestas, hasta concluir con un análisis financiero sobre la aplicación de la propuesta.

Dentro de los resultados obtenidos se define la documentación estandarizada de las políticas propuestas, sus procesos, diagramación, resultados de simulaciones y análisis financiero; esto con el objetivo de que la organización cuente con la documentación necesaria para implementar la propuesta.

El documento finaliza con una serie de recomendaciones realizadas sobre todo el proceso llevado a cabo para la finalización de la propuesta, así como un listado de conclusiones sobre los descubrimientos más relevantes de la investigación.

Palabras clave: política, seguridad, antivirus, marco de referencia, usuarios, COBIT 5, BPM.

Abstract

This document aims to show the analysis carried for select and propose information security policies that promote an articulated management of security processes in all the organization's collaborators.

This project is based on the alternative methodology, which entails the demonstration of three dimensions: epistemological, ontological, and axiological. Also, three phases were defined that comprise the activities necessary for the understanding and solution of the problem. The first phase includes the delimitation of the policies that will be part of the proposal, as well as the processes that each of these policies contains. Along with, details such as the As-Is diagram of the current situation and the explanation and measurement of improvement opportunities for each policy are included. The main objective of the second phase is to establish the gap between the current situation and the COBIT 5 framework, as well as the diagramming of the processes and policies resulting from the gap analysis. And in the last phase, the simulation of the policies on which it can be simulated is carried out, and then a measurement of the effectiveness of the proposed policies is carried out, concluding with a financial analysis.

As results obtained, standardized documentation of the proposed policies, their processes, simulations, and financial analysis is defined, with the objective that the organization has the necessary documentation for the implementation of the proposal.

This document ends with recommendations of the entire process carried out to finalize the proposal, as well as a list of conclusions on the most relevant results of the investigation.

Key words: policy, security, antivirus, framework, users, COBIT 5, BPM.

Tabla de Contenidos

ati

Índice de Figuras

Índice de Tablas

Nota Aclaratoria

Género[1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española en relación con el uso del "género inclusivo". Al mismo tiempo, se aclara que estamos a favor de la igualdad de derechos entre los géneros.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

1. Introducción

1.1. Descripción General

Actualmente, el comercio digital ha pasado a formar parte de la vida cotidiana de la industria y de las personas. Para una empresa es importante mantenerse al día en aspectos tecnológicos, pues esto le permite aspirar a un innumerable mercado de clientes. Pero, así como se toman en cuenta los beneficios de la era digital es importante también identificar los peligros que se pueden enfrentar.

Como parte de este auge digital nace Xumtech. Esta es una empresa formada hace cinco años y que tiene como principal objetivo proveer a sus clientes herramientas tecnológicas que les brindan beneficios de automatización de procesos, transformación digital, mercadeo digital de productos, entre otros. El ser un proveedor de servicios digitales no lo hace estar exento de los peligros que rodean la web. Al estar expuesta a un rápido crecimiento en su cartera de clientes, Xumtech requiere de mecanismos que le provean de políticas de seguridad actualizadas para resguardar tanto su información como la de sus clientes, además de la integridad física de los equipos tecnológicos de la organización.

En este proyecto se realizará el análisis de la situación actual de las políticas de seguridad y procesos de la empresa Xumtech; este es el primer paso para definir la brecha existente entre lo que se tiene hoy y lo que dictan las buenas prácticas del mercado. Las oportunidades de mejora identificadas se usarán para proponer una actualización de las políticas de seguridad y de sus procesos asociados, para posteriormente evaluar el nivel de efectividad de las políticas y procesos de seguridad propuestos con respecto a la situación actual.

1.2. Antecedentes de la empresa

En esta sección se brinda el contexto acerca de Xumtech como empresa, así como proyectos similares, el problema por tratar y el equipo de trabajo.

1.2.1. Descripción de la organización

La empresa Xumtech nació en el 2016 como una PYME dedicada a brindar innovación y transformación digital a las empresas que lo requerían. Cuenta en su cartera con una base de clientes nacionales e internacionales, entre los que se incluyen compañías de logística, financieras y de manufactura.

Mediante el lema de "hacer que las tecnologías de información más innovadoras sean accesibles a organizaciones menos familiarizadas con la informática y computación" (Suum Technologies, 2020), brinda servicios de consultoría enfocada en productos Oracle, siendo parte de esta empresa desde su nacimiento.

Desde el punto de vista organizacional la empresa cuenta con una modalidad 100% virtual, por lo que sus colaboradores se encuentran ubicados en muchas partes del territorio nacional e internacional. Estos colaboradores se organizan por medio de "Tribus", que consisten en grupos enfocados en la implementación de uno o varios proyectos para uno o varios determinados clientes. Cada tribu tiene, a su vez, los roles de consultor, líder técnico y, de ser necesario, dueño de producto. Estos roles se encuentran definidos en Tabla 1. Equipo de trabajo.

En los últimos años, la empresa se ha visto expuesta a un crecimiento tanto en su cartera de clientes nacionales e internacionales como en las iniciativas enfocadas a soporte, por lo que aspectos como aumentar el número de colaboradores, la necesidad de contar con oficina y la actualización de su imagen corporativa, son los próximos pasos en el proceso de crecimiento.

1.2.2. Misión, Visión y equipo.

A continuación, se describe la misión, la visión y el equipo de trabajo de la empresa Xumtech.

- **Misión**

"Hacer que las tecnologías de información más innovadoras sean accesibles a todas las organizaciones sin importar su tamaño o familiaridad con la tecnología" (Suum Technologies, 2020).

- **Visión**

Según Suum Technologies (2020) la visión de la organización se basa en los siguientes ejes:

  - Crecimiento interno de la organización.
  - Desarrollo de relaciones cercanas con los clientes.
  - Crecimiento profesional y personal de los colaboradores.
  - Crecimiento financiero.

- **Equipo de trabajo**

En la Tabla 1. Equipo de trabajo, se describen los roles de los participantes que integrarán este proyecto. Además, se detallarán algunas de las funciones y actividades desarrolladas por los roles en la organización. La selección de cada uno de estos autores está premeditada por políticas internas de desarrollo de proyectos académicos, así como por la asignación de personal relacionado a los distintos proyectos activos de la empresa.

Tabla 1. Equipo de trabajo

Rol	Funciones del rol	Funciones del rol en el proyecto
Gerente General	• Tareas administrativas. • Tareas de representación de la empresa. • Tareas de mejora continua. • Funciones comerciales, ventas y cotizaciones.	• Gestión de aspectos administrativos. • Juicio de experto sobre procesos de la empresa. • Validar el cumplimiento de los intereses de la organización.
Dueño de producto	• Gestión de proyectos e iniciativas de un determinado cliente. • Planeación de rutas y cronogramas de implementación. • Gestión del diseño de solución del proyecto. • Labores de consultoría.	• Gestión de aspectos administrativos. • Rol encargado de aceptar la propuesta. • Juicio de experto sobre procesos de la empresa.
Líder técnico	• Gestión del equipo de trabajo (Tribu). • Gestión de documentación técnica y funcional. • Seguimiento y asignación de tareas de implementación. • Gestión de casos de soporte.	• Rol del estudiante que desarrollará el proyecto.
Consultor	• Realización de tareas de implementación. • Gestión de documentación técnica y de gestión de los proyectos.	• Sujetos de investigación para el proyecto.

Fuente: Elaboración propia, 2021.

1.2.3. Trabajos similares realizados dentro y fuera de la organización

En esta sección se detallan proyectos internos y externos a la organización que serán tomados como referencia para el desarrollo de este proyecto.

Como punto por considerar, los proyectos internos de la organización tienen restricciones sobre el uso de documentación y datos de estos proyectos, pues dependen de acuerdos de confidencialidad que impiden su anexo a este proyecto y el uso limitado de información.

Entre los proyectos externos a la organización se tienen los siguientes.

- **"Propuesta de mejora para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, basado en el estándar ISO/IEC 27002:2005" (Sierra, 2014)**

  En este proyecto el autor toma las políticas de seguridad de la información del Banco Central de Costa Rica y las contrasta contra el estándar ISO/IEC 27002:2005; deja en evidencia la brecha existente e identifica oportunidades de mejora cuyo principal objetivo es alinear a la organización con el estándar mencionado anteriormente.

  En cuanto a su relación con este proyecto, el autor aborda el mejoramiento de políticas de seguridad mediante la utilización de un estándar de buenas prácticas del mercado, lo cual se adapta a la situación problemática y objetivos del proyecto por realizar.

- **"Propuesta de solución para el proceso de seguramiento de la calidad de software en la empresa SUUM Technologies apoyado en estándares y buenas prácticas de la industria" (Jiménez, 2020)**

  Mediante la utilización de metodologías para el análisis de procesos, el autor identifica oportunidades de mejorar el proceso de aseguramiento de la calidad con el que cuenta la organización. Las oportunidades de mejora fueron identificadas tomando en cuenta estándares y buenas prácticas de la industria.

Este proyecto se relaciona con el presente debido a que aborda el mejoramiento de procesos en la empresa SUUM Technologies, la misma empresa en la cual se desarrollará este trabajo final de graduación.

En cuanto a los proyectos internos de la organización se cuenta con la siguiente referencia:

- **"Estándares de diseño y construcción" elaborado por Sally Ureña**
  Manual de estándares y políticas utilizado por los colaboradores de la organización para estandarizar la configuración de ambientes y el desarrollo de código en las distintas iniciativas. Plantea un uso adecuado de recursos tecnológicos, así como la generación de una traza que permita identificar el código y configuraciones realizados por colaboradores de la organización.

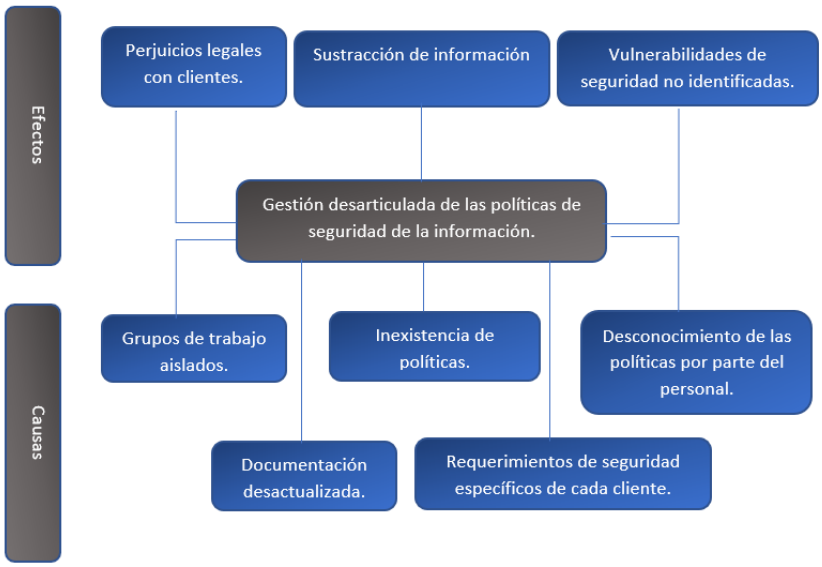
1.3. Planteamiento del problema

En esta sección se describe la situación problemática encontrada, así como las causas y efectos identificados. Además, se detallan algunos beneficios esperados como resultado del proyecto planteado.

1.3.1. Situación problemática

Para definir la situación problemática se utilizó la herramienta diagrama de árbol de problemas, con el cuál se definieron las causas y los efectos involucradas en el problema central de la compañía (Ver Ilustración 1. Árbol de problemas sobre la gestión desarticulada de las políticas de seguridad de la información).

Ilustración 1. Árbol de problemas sobre la gestión desarticulada de las políticas de seguridad de la información



Fuente: Elaboración propia, 2021

Como parte de las causas de la problemática identificada en el árbol de problemas, destaca el método de trabajo utilizado por la organización. La empresa cuenta con grupos de colaboradores llamados *tribus.* Cada tribu tiene a cargo el desarrollo de un determinado proyecto para cada cliente. Entre los distintos proyectos surgen nuevas políticas de seguridad con el

objetivo de cumplir con requerimientos de un cliente específico, sin embargo, esto provoca problemas relacionados con la ausencia interna de estandarización de las políticas de seguridad. Dicha falta de estandarización genera en los miembros de la organización desconocimiento sobre las políticas de seguridad aplicadas en otras tribus y que podrían ser de provecho para la empresa en general. Sumado a esto, en cada tribu se cuenta con una serie de políticas que permiten cumplir con las exigencias mínimas de seguridad de la información planteadas por los clientes, tanto en cláusulas de contratos legales, como en requerimientos solicitados por las empresas durante la etapa de licitación de una determinada iniciativa de venta.

Además, la organización se encuentra en una etapa de alto crecimiento que la reta a contar con políticas de seguridad que protejan la propiedad intelectual, información de clientes y datos relacionados con la conformación de nuevos clientes como negociaciones, contratos y montos económicos. Debido al crecimiento que experimenta la empresa y a la falta de herramientas que agrupen las políticas de seguridad organizacionales, se ve en la necesidad de llevar a cabo la actualización de políticas de seguridad las cuáles se deben adaptar tanto los colaboradores existentes como los que están por ingresar, esto para mitigar cualquier tipo de riesgo relacionado a malas intenciones del recurso humano o a malas prácticas que pongan en riesgo las actividades cotidianas de la empresa.

Lo anteriormente mencionado pone a la empresa en potenciales riesgos, como el robo de propiedad intelectual desarrollada por la organización, así como de datos pertenecientes a los clientes. Además, esta gestión desarticulada de la seguridad puede generar el incumplimiento de cláusulas legales que provoquen perjuicios económicos y poner en riesgo el prestigio desarrollado ante el mercado de clientes.

Si bien el problema de no contar con un estándar de las políticas de seguridad es amplio para el tiempo disponible, en este proyecto se pretende, mediante un listado de políticas resultantes del análisis de la situación actual y de un proceso de priorización del conjunto de políticas y procesos obtenidos, acopiar un número acotado de políticas de seguridad. Los procesos se

incluirán en cada una de las políticas, según corresponda, tomando como base la priorización realizada y las buenas prácticas.

1.3.2. Justificación del proyecto

Esta sección tiene como objetivo definir, mediante marcos de referencia, conceptos y tecnologías, las razones por las cuales la situación problemática expuesta anteriormente puede ser abordada por un estudiante de administración de tecnología de información.

Actualmente, el auge de las empresas que desean mejorar sus procesos tomando la tecnología de información como precursor, son muchas, por lo cual resalta la importancia de disponer de ventajas competitivas que ubiquen a las empresas por encima de la competencia. En este caso, Xumtech ha crecido gracias a la confianza que han mostrado los clientes hacia su gestión de proyectos y al prestigio creado a partir de los proyectos realizados y los resultados obtenidos post producción. Como parte de su crecimiento, la empresa desea reforzar sus procesos de seguridad mediante la actualización de las políticas, esto con el fin de apuntar a un mercado más exigente y de revalidar su prestigio ante su cartera de clientes. Dicho esto, un estudiante de ATI desde el área de desarrollo del TFG de Auditoría, seguridad y riesgos, puede brindar a la empresa Xumtech políticas de seguridad actualizadas y basadas en buenas prácticas de la industria que les permita continuar con el crecimiento esperado.

Como parte de los primeros pasos, es necesario conocer el universo de políticas por analizar en este proyecto, decisión que se debe tomar en mutuo acuerdo con la contraparte de la organización; en este proceso un ATI es de gran ayuda, debido a su conocimiento actualizado sobre la industria y sobre las tendencias del mercado.

Posteriormente a esto, se debe tener conocimiento sobre el estado actual de los procesos de seguridad donde se involucran las políticas seleccionadas. Para un mejor análisis se utilizará la notación BPM, la cual permitirá conocer el paso a paso de los procesos y políticas de seguridad involucradas.

Para identificar la brecha entre las políticas actuales y las mejores prácticas la organización requiere asesoría sobre cuáles marcos de referencia se adaptan mejor a su cultura organizacional, por tanto, un profesional en tecnologías de información tiene las habilidades suficientes para recomendar estándares del mercado que se adapten a lo solicitado por la empresa. Según lo observado, como la información es uno de los activos más importantes de la organización, las políticas deben ir dirigidas a la protección y correcta manipulación de este activo, por tanto, se propone como base el triángulo CIA el cual, según la Central Oregon Community College (s.f) asegura la confidencialidad, disponibilidad e integridad de la información.

Además, con el fin de velar por la correcta evolución de la empresa en cuanto a la protección de su información, es de vital importancia contar con procesos de análisis de las medidas de seguridad, las cuales permitan identificar nuevas amenazas que pongan en riesgo la confidencialidad e integridad de la información. Como mecanismo de mejora continua para las políticas de seguridad se plantea el ciclo de Deming, que según Gutierrez (2010) mediante las actividades planear, hacer, verificar y actuar, posibilita mejoras a procesos.

Sumado a lo anteriormente mencionado, es necesario incluir durante el periodo de desarrollo del proyecto habilidades propias de un futuro profesional en administración de tecnología de información. Entre las habilidades mencionadas destacan, por ejemplo, la administración de proyectos para gestión de cronograma, cambios que se puedan presentar y para velar por el alcance propuesto. Además, se vislumbra la necesidad de contar con habilidades blandas para una adecuada interacción con los colaboradores de Xumtech.

1.3.3. Beneficios esperados o aportes del Trabajo Final de Graduación

Tras la realización del proyecto que pretende atender la problemática citada anteriormente se espera obtener los siguientes beneficios:

- Estandarización de las políticas de seguridad para el acceso y conocimiento general de las tribus de la organización sobre las políticas de seguridad y procesos asociados existentes.
- Medición de las políticas en términos de oportunidades de mejora mediante la utilización de rubros definidos para la organización.
- Medición de la efectividad de las políticas nuevas y existentes utilizando rubros definidos según laos estándares de efectividad de la organización.
- Medición del nivel de madurez de la organización en seguridad informática basado en los Controles CIS, lo que permite a la organización verificar su posición actual y a que puede aspirar

1.4. Objetivos del Trabajo Final de Graduación

1.4.1. Objetivo General

- Elaborar una propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech en un lapso de dieciséis semanas para la estandarización de los procesos asociados a las políticas de seguridad utilizadas en la organización.

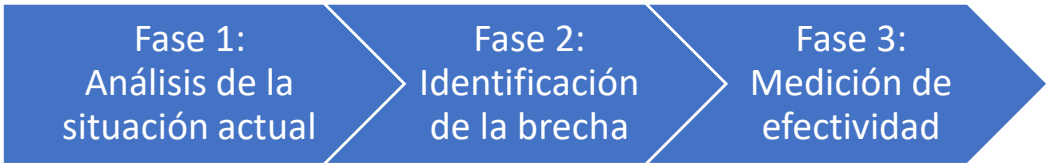
1.4.2. Objetivos Específicos

- Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.
- Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria
- Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis financiero para la validación de la efectividad de las mejoras propuestas.

1.5. Alcance

En esta sección se detallan las distintas etapas por las que pasará el proyecto, con el fin de describir lo contemplado dentro del alcance del proyecto.

Ilustración 2. Fases del proyecto



Fuente: Elaboración propia, 2021.

Tal y como se presenta en la Ilustración 2. Fases del proyecto, para tener un mejor contexto del ambiente, procesos y políticas de seguridad con los que cuenta la empresa, se iniciará el proyecto realizando un análisis de la situación actual mediante la revisión de los documentos relacionados con la seguridad de la organización. Teniendo contexto sobre la organización, el paso es la selección del conjunto de políticas sobre las cuales se desarrollará el proyecto. Estas políticas deben ser de gran impacto para la organización, pero a la vez deben poder desarrollarse durante las dieciséis semanas de aplicación del proyecto. Además, como parte de la Fase 1, se requiere conocer la perspectiva del recurso humano sobre el uso en la organización de las políticas seleccionadas; esto, mediante la aplicación de los instrumentos para recopilar información, definidos para los distintos roles de la organización. Al realizar este proceso investigativo, se contará con la perspectiva del recurso humano sobre las políticas de seguridad que se utilizan actualmente, así como de la cotidianidad y profundidad con que estas son aplicadas por los distintos colaboradores pertenecientes a las tribus de trabajo de la compañía. Posterior a esto, se procede a la generación de diagramas As-Is, utilizando la notación BPMN que permitan analizar de mejor forma las políticas identificadas como prioritarias y dejar evidencia de la situación actual de ellas. Estos diagramas serán parte de los entregables a la empresa, dado que actualmente no cuentan con insumos de este tipo. Paso siguiente, las políticas seleccionadas y sus procesos deben ser sometidos al análisis de si se consideran o no como oportunidad de

mejora; esto, realizado según lo definido en la metodología de investigación del proyecto y según el enfoque seleccionado.

Para la Fase 2, se debe identificar la brecha existente tomando como referencia los diagramas *As-Is* y comparándolo contra las buenas prácticas de la industria. La etapa de identificación de la brecha abarca la delimitación de los procesos que se abarcarán en cada una de las políticas, esto según los resultados obtenidos de la aplicación de los instrumentos para recopilar información. Dicha brecha será evidenciada mediante la realización de diagramas *To-Be* que proyecten los procesos que se proponen y las actualizaciones identificadas sobre los procesos ligados a las políticas elegidas. Estos diagramas *To-Be* formarán parte de los entregables finales del proyecto como evidencia de la brecha identificada durante el desarrollo de este. Una vez realizados los diagramas *To-Be*, se deben actualizar las políticas seleccionadas como prioritarias, según lo identificado en el análisis de la brecha. Luego, se propondrá un insumo que cuente con la recopilación de las políticas seleccionadas como prioritarias y previamente actualizadas, con base en las buenas prácticas seleccionadas. Este entregable tiene como objetivo ser una guía para el control de políticas de seguridad apegadas a la realidad de la empresa y las buenas prácticas de la industria.

Para la Fase 3, se desea tener visibilidad sobre los tiempos asociados a los procesos de las políticas de seguridad y contar con información relevante para utilización en la empresa, por tanto, se aplicarán simulaciones sobre los procesos propuestos para las políticas seleccionadas. De estas simulaciones quedará evidencia escrita mediante el análisis que se realiza de los resultados obtenidos. Para finalizar, se realizará un análisis de la efectividad de las propuestas realizadas. Este análisis será utilizado para evaluar el beneficio obtenido por la organización según los rubros definidos en la metodología de investigación del proyecto. Se dejará evidencia de los resultados obtenidos mediante un documento que exponga los detalles del análisis efectuado, el cual formará parte de los entregables de este proyecto.

1.6. Supuestos

Esta sección deberá indicar explícitamente los factores o elementos que usted asume se cumplirán o serán ciertos en la realización del proyecto.

1. Se contará con acceso a documentos relacionados a medidas, políticas o manuales de seguridad. No se pondrán limitaciones de acceso a documentación de seguridad que pueda servir como insumo para el desarrollo de este proyecto.
2. Los colaboradores de la empresa Xumtech se mostrarán dispuestos a colaborar en los grupos focales, encuestas y de los ejercicios que se desarrollen para este proyecto. Además, se mostrarán anuentes a colaborar con cualquier tipo de guía o información requerida durante cualquiera de las etapas de desarrollo del proyecto.

1.7. Entregables

A continuación, se describen los entregables asociados a cada objetivo del proyecto, divididos en entregables de producto y entregables académicos.

Para los entregables de producto que deben ser aportados a la organización, se tomaron en cuenta los objetivos específicos detallados anteriormente. Por tanto, cada objetivo específico cuenta con los siguientes entregables

- Documentos BPM con los diagramas As-Is sobre la situación actual de los procesos y políticas de seguridad de la información. Este documento BPM contendrá un análisis de hallazgos de la situación actual, listado y priorización de políticas de seguridad, así como los documentos de gestión que evidencien la realización de los grupos focales, minutas sobre las reuniones realizadas y pruebas documentales de cualquier cambio que se considere sobre el proyecto.
- Documentos BPM con los diagramas To-Be que permitan evidenciar la brecha existente entre las mejores prácticas de la industria y las políticas seleccionadas del listado de priorización. Este documento dispondrá de un análisis en el cual se plasmarán las oportunidades de mejora identificadas a través de la comparación entre las buenas prácticas y la situación actual.
- Propuesta de las políticas de seguridad y procesos asociados.
- Documento de análisis costo beneficio de las políticas actualizadas basado en la situación actual, el listado de priorización realizado durante la etapa de situación que prevalece y los resultados obtenidos de las simulaciones realizadas.

En cuanto al entregable académico, se brindará el documento estipulado en el reglamento sobre trabajo final de graduación para estudiantes de la carrera de Administración de Tecnología de Información. La entrega y revisión de este documento se realizará de forma parcial, determinada por el número de objetivos y lapso definidos por el tutor asignado.

1.8. Limitaciones

En este apartado se detallan los aspectos que se pueden convertir en limitantes para los distintos entregables que abarca este proyecto.

1. **Confidencialidad de la información.**

   Xumtech trabaja con clientes que disponen de altos niveles de confidencialidad de la información involucrada en los distintos proyectos desarrollados, convirtiendo esto en una limitante para exposición de datos reales, nombres de clientes, proyectos desarrollados, entre otros. Por tanto, para el desarrollo de este proyecto no se utiliza información relacionada con clientes de la empresa o información interna que ponga en riesgo información de clientes.

2. **Disponibilidad de los colaboradores.**

   Los actores de la empresa involucrados en este proyecto dispusieron de una porción limitada de tiempo de su jornada laboral para la realización de este proyecto, por tanto, se tomaron acciones como la solicitud de las sesiones mediante cita previa y la realización de actividades fuera de horario laboral.

2. Marco Conceptual

Este capítulo tiene como principal objetivo brindar una base conceptual que permita abordar el problema planteado, además, enumera los marcos de trabajo utilizados para la solución de mejora.

Según Reidl (2012) el marco conceptual es generado a partir de supuestos teóricos del investigador con los que pretende darle sustento a su investigación, también con límites claros basados en la literatura consultada.

Por tanto, en este capítulo se abordan conceptos básicos de gestión de procesos de negocio, metodología *BPMN* para el análisis de procesos y marcos de trabajo utilizados.

2.1 CIS

CIS es el acrónimo de *Center for Internet Security* (en español Centro para la Seguridad en Internet). Según CIS (s.f) es una organización sin fines de lucro que envuelve numeroso número de investigadores encargados de modelar estrategias de seguridad para los entornos informáticos de las empresas.

2.1.1 Controles CIS

Como parte de los marcos de referencia del *CIS* se encuentran los *CIS Controls* (en español Controles CIS), los cuales CIS (2019) define como acciones priorizadas que forman un marco de referencia utilizado por las organizaciones, cuyo principal objetivo es mitigar los ataques más comunes presentados en redes y sistemas.

La aplicación de los controles CIS está delimitada por los *CIS Controls Implementation Groups* (en español Grupos de implementación de los Controles CIS). En la Ilustración 3. Grupos de implementación CIS, se muestra cada uno de los grupos de implementación existentes en los Controles CIS. Para CIS (2019) estos grupos de implementación permiten aplicar controles y subcontroles basados en el tamaño y recursos disponibles por la organización en temas de ciberseguridad. En total, son tres grupos de implementación disponibles que se definen de la siguiente manera:

- **Grupo de implementación 1:** El *IG1* (por sus siglas en inglés) está enfocado en organizaciones pequeñas con conocimiento básico, personal limitado y recursos básicos dedicados a la protección de los activos de *TI. CIS* cataloga la información sensible de la empresa como mayoritariamente financiera y de los empleados. Además, las organizaciones pertenecientes a este grupo deben aplicar los controles y subcontroles pertenecientes a este grupo, con el fin de protegerse de ataques cibernéticos no dirigidos.
- **Grupo de implementación 2:** El *IG2* (por sus siglas en inglés) abarca las organizaciones que tienen personal dedicado a administración y protección de la infraestructura de *TI.* Además, menciona que las empresas pertenecientes a este grupo a menudo administran información sensible de clientes y empresas. Por tanto, los controles y subcontroles de este grupo de implementación están relacionados con recomendaciones sobre ejecución y mejora de tareas de seguridad de la infraestructura.
- **Grupo de implementación 3:** El *IG3* (por sus siglas en inglés) menciona estar dedicado a empresas que tienen entre sus colaboradores a expertos en las áreas de ciberseguridad. Otro factor importante para este grupo de implementación es la alta disponibilidad a la que deben estar sus servicios, los cuales están atados a contratos y a regulaciones legales. Los controles y subcontroles para este grupo están enfocados en lograr que el equipo de trabajo encargado de la seguridad de la infraestructura de *TI* trabaje de forma integral y abarcando cualquier aspecto que ponga en riesgo los activos de las empresas.

Ilustración 3. Grupos de implementación CIS

	**Definiciones**	1	2	3
	Los subcontroles CIS para entornos de comerciales pequeños y de teletrabajo donde la sensibilidad de los datos es baja generalmente se incluirán en IG1. Recuerde, cualquier paso de IG1 también debe ser seguido por organizaciones en IG2 e IG3.	●	●	●
	Son subcontroles de CIS centrados en ayudar a los equipos de seguridad a administrar información confidencial de clientes o empresas, y se incluyen en IG2. Los pasos de IG2 también deben ser seguidos por organizaciones en IG3.		●	●
	Son subcontroles de CIS que reducen el impacto de los ataques dirigidos y sofisticados. Estas empresas normalmente caen en IG3. Es posible que las organizaciones IG1 e IG2 no puedan implementar todos los subcontroles IG3.			●

Fuente: Elaboración propia. Adaptación al español de CIS, 2019.

Del total de controles CIS disponibles, se seleccionan cuatro que se adaptan a lo requerido para el proyecto. Estos controles seleccionados corresponden al Grupo de implementación 1, definido anteriormente, debido a que este grupo de implementación corresponde a recomendaciones para organizaciones pequeñas. CIS (2019) define estos controles como:

- Control CIS 8: Defensas contra software malicioso.

  Brinda herramientas para el control e instalación de código malicioso. Vela por la automatización de procesos de actualización de los sistemas de defensa contra programas malignos.
- Control CIS 13: Protección de datos.

Establece subcontroles para prevenir la filtración de información, mitigar cualquier filtración que se presente y garantizar la integridad de la información.

- Control CIS 4: Control y uso de privilegios administrativos.

  Provee procesos para controlar los accesos brindados a los distintos colaboradores de la organización, así como controles para nuevos accesos.

- Control CIS 2: Inventario y control de los activos de software.

  Detalla los controles recomendados para la gestión y conocimiento de los activos de software con los que cuenten las organizaciones. Brinda herramientas para la vigilancia y para exponer el uso y la existencia de dichos activos.

2.2 COBIT 5

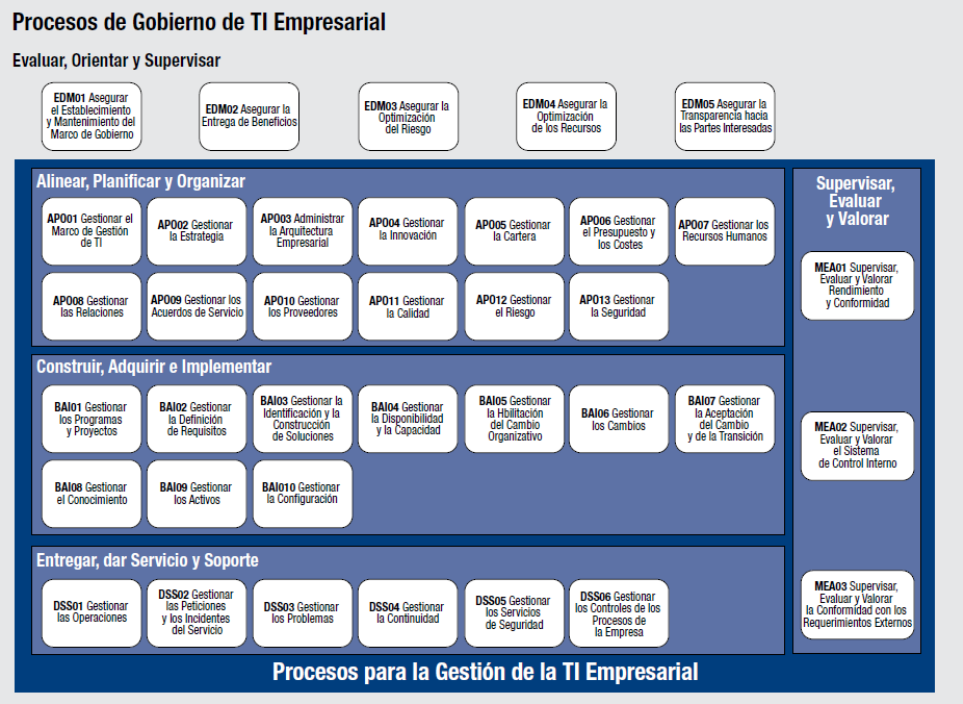
Encalada y Loda (2016) definen COBIT 5 como un marco de gobierno de las tecnologías de información que tiene como fin brindar herramientas a las organizaciones para que se puedan establecer relaciones entre los riesgos identificados en el área de la seguridad de la información y los objetivos de control a nivel directivo.

Según ISACA (2012) el modelo de referencia sobre el cual está basado COBIT 5 pretende que las organizaciones implementen de forma paralela procesos relacionados al gobierno de *TI* y procesos enfocados en la gestión del entorno de *TI*. Para una mejor referencia sobre los procesos de gobierno y de gestión, ISACA (2012) menciona que cada uno de estos cubre:

- Los procesos de gobierno involucran la evaluación de estrategias, además, están relacionados con la optimización del riesgo y la entrega de valor. Para esto, se definieron las prácticas *EDM* (Evaluar, Orientar y Supervisar), que incluyen cinco procesos en total.
- Los procesos de gestión contienen cuatro dominios, brindando cobertura de *TI* extremo a extremo.

En la Ilustración 4. Procesos de gobierno y gestión COBIT 5, se muestran los procesos COBIT 5 de gestión y de gobierno.

Ilustración 4. Procesos de gobierno y gestión COBIT 5



Fuente: ISACA, 2012.

Para el desarrollo de este proyecto, se utiliza el dominio DSS05 Gestionar los servicios de seguridad, que forma parte de los procesos de gestión DSS (Entregar, dar Servicio y Soporte).

Según ISACA (2012) el proceso DSS05 Gestionar los Servicios de Seguridad, tiene como objetivo proteger la información de la organización, esto para mantener mínimos niveles de riesgo. Además, procura que se brinde una correcta administración de los privilegios de acceso, para una adecuada supervisión de la seguridad.

Entre las prácticas claves del proceso que se aplican en este proyecto, ISACA (2012) enumera las siguientes:

BAI09.01 Identificar y registrar activos actuales

Permite que las organizaciones cuenten con un registro actualizado de todos aquellos activos de TI con los que se cuente. Esto brinda beneficios como la alineación de las estrategias involucradas en gestionar la configuración y aspectos financieros. En la Ilustración 5. Actividades de

BAI09.01 Identificar y registrar activos actuales, se muestran las actividades recomendadas por el marco de referencia.

Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales

Actividades
1. Identificar todos los activos en propiedad en un registro que indique el estado actual. Mantener su alineación con los procesos de gestión de cambios y de la configuración, el sistema de gestión de la configuración y los registros contables financieros.
2. Identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos.
3. Verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación, incluyendo la utilización de herramientas software de descubrimiento.
4. Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles).
5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.
6. Asegurar la contabilización de todos los activos.

Fuente: ISACA (2012).

DSS05.04 Gestionar la identidad del usuario y el acceso lógico

Faculta a los actores de la organización para evaluar que los usuarios cuenten con los permisos de acceso que se adapten a los requerimientos del negocio. Además, faculta a otras secciones, en caso de ser necesario, en tareas de evaluación de accesos y permisos. En la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, se evidencian las actividades recomendadas.

Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico

Actividades
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
2. Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.
3. Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.
5. Segregar y gestionar cuentas de usuario privilegiadas.
6. Realizar regularmente revisiones de gestión de todas las cuentas y privilegios relacionados.
7. Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones de negocio, infraestructura de TI, operaciones de sistema, desarrollo y mantenimiento) son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario.
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.

Fuente: ISACA (2012).

DSS05.01 Proteger contra software malicioso (*malware*)

Busca la implementación de controles de seguridad enfocados a la detección, prevención y corrección de amenazas producidas por software malicioso. En la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware) se enumeran todas las actividades recomendadas.

Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware)

Actividades
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing).
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.

Fuente: ISACA (2012).

2.3 Política de seguridad.

Para Duque (2002) se puede interpretar una política de seguridad como un conjunto de pasos y condiciones por seguir que determinan cómo una empresa puede gestionar información sensible relacionada con clientes, accesos a sistemas o datos financieros propios.

Para el desarrollo integral de una política de seguridad en una organización, Duque (2002) define que se debe tomar como soporte la situación actual del entorno organizacional, para la construcción de políticas que se apeguen a los recursos, riesgos y herramientas con las cuales se cuente. Asimismo, es importante que se logre vincular todos los sectores involucrados en las políticas por desarrollar, esto con la finalidad de evitar que la resistencia al cambio comprometa la razón de ser de las políticas.

Además, Duque (2002) señala que una política de seguridad debe cumplir dos objetivos principales, los cuales son:

- Hacer saber a los colaboradores de la organización sobre los deberes y requisitos por cumplir respecto de la seguridad de la información y tecnología de la empresa.
- Brindar un paso a paso por seguir ante amenazas y problemas de seguridad.

2.4 Proceso

El término *proceso* se define, según Mallar (2010), como una agrupación de pasos o actividades relacionadas entre sí y con una secuencia específica, que se identifican por recibir insumos, productos o servicios que posteriormente se convertirán en determinadas salidas, cuyo propósito es brindar valor a la organización.

Según Mallar (2010) se puede identificar un proceso porque cuenta con los siguientes tres elementos:

- Entradas: Se refiere a materia prima, personal activo o información por procesar que debe ser transformada.

- Factores que transforman: Incluye tanto factores humanos, relacionados con actividades complejas como planificación, organización y dirección, así como factores de apoyo: infraestructura tecnológica.
- Flujo real de procesamiento: Enfocado al tipo de transformación que se realiza sobre las entradas, por ejemplo: transformación física, transporte de objetos, modificaciones jurídicas o legales, entre otras.
- Salidas: Resultado final de la aplicación de los factores que transforman sobre las entradas y mediante la utilización del flujo real de procesamiento. Las salidas pueden ser bienes físicos o servicios.

Dada la existencia de múltiples tipos de procesos, este proyecto utiliza los denominados como procesos de negocio, los cuales la CAIGG (2016) define como un número de acciones ejecutadas en un orden específico, estrechamente relacionadas con los objetivos estratégicos de la organización. Dicho de otra forma, los procesos de negocio manifiestan el hacer cotidiano de la organización.

2.5 Gestión de procesos de negocio (BPM)

Garimella et al. (s.f) definen *BPM,* por sus siglas en inglés que significan *Business Process Management,* como las herramientas y tecnologías usadas para gestionar y analizar procesos de negocio. Además, señalan que el principal objetivo de le gestión de procesos de negocio es que las personas de negocio, en conjunto con profesionales en tecnología, promuevan procesos efectivos y que entreguen el máximo valor al negocio.

Además, los autores señalan que el *BPM* engloba todas las aristas que intervienen en un proceso, por ejemplo: sistemas, proveedores, clientes, entre otros.

Asimismo, Garimella et al. (s.f) señalan que el *BPM* se dirige al mundo empresarial gracias a sus tres dimensiones esenciales, las cuales se definen a continuación:

- La dimensión de valor: Tomando al negocio como el actor principal, se menciona que la gestión de procesos de negocio crea valor, de forma paralela, para los clientes y

para los *stakeholders* de los procesos. Además, se justifica la creación de valor basado en la capacidad de alineamiento que tiene *BPM* entre los objetivos estratégicos y las actividades operacionales.

- La dimensión de transformación: Esta dimensión justifica la creación de valor en los negocios mediante la capacidad de transformación que tiene un proceso. Un proceso de negocio recibe recursos o materiales, según su naturaleza, y su principal objetivo es generar productos o servicios que posteriormente serán utilizados por el negocio para generar valor para sí mismo y para sus socios.
- La dimensión de capacitación: Tomando la gestión como eje principal, esta dimensión señala que una correcta gestión de los actores principales de los procesos de negocio promueve la realización y cumplimiento de los objetivos estratégicos y genera el anhelado éxito empresarial.

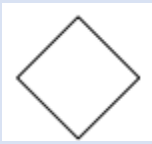
2.6 BPMN

La notación de gestión de procesos de negocios (*Business Process Management Notation*, conocido como BPMN, por sus siglas en inglés), es definida por White (2004) como un estándar que tiene como fin disminuir la brecha existente entre el diseño comercial y la implementación de los procesos. Consiste en una notación de fácil comprensión para cualquier usuario del proceso, desde las personas de negocio hasta los especialistas técnicos que se encargan de la implementación de dichos procesos.

Para la generación de diagramas bajo la notación *BPMN,* White (2004) menciona la existencia de cuatro categorías de elementos, los cuáles son:

- Objetos de flujo, los cuales se detallan en Tabla 2. Objetos de flujo.
- Objetos de conexión, expuestos en Tabla 3. Objetos de conexión
- Carriles, como los mencionados en Tabla 4. Carriles.
- Artefactos, tomando como ejemplo los señalados en Tabla 5. Artefactos

Tabla 2. Objetos de flujo

Elemento	Simbolo	Definición
	Evento	Ocurre durante el transcurso del proceso. Generalmente tiene una causa disparadora.
	Actividad	Acción que se realiza dentro de un proceso. Puede ser atómica o compuesta.
	Compuerta	Determina las decisiones que se llevan dentro del proceso, la bifurcación y la unión de flujos.

Fuente: Adaptado de Introduction to BPMN, por Stephen A. White, 2004.

Tabla 3. Objetos de conexión

Elemento	Símbolo	Definición
	Secuencia	Muestra el orden secuencial en el que se ejecutan las actividades del proceso.
	Mensaje	Representa el intercambio de mensajes entre dos participantes del proceso.
	Asociación	Asociación de textos, datos y otras fuentes con los objetos de flujo.

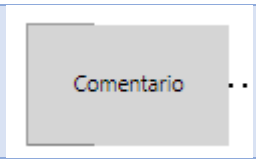
Fuente: Adaptado de Introduction to BPMN, por Stephen A. White, 2004.

Tabla 4. Carriles

Elemento	Símbolo	Definición
	*Pool*	Representa un participante de un proceso. Se refiere a un actor en específico, área, departamento, entre otros.
	*Lane*	Son carriles que se utilizan para categorizar las actividades. Dividen un *Pool* en distintas secciones.

Fuente: Adaptado de Introduction to BPMN, por Stephen A. White, 2004.

Tabla 5. Artefactos

Elemento	Símbolo	Definición
	Objeto de datos	Muestra cuando una actividad tiene datos como entrada o salida.
	Grupo	No afecta el flujo del proceso. Consiste en agrupaciones de actividades con fines de análisis o ilustrativos.
	Comentario	Información necesaria a aclarar para una determinada actividad.

Fuente: Adaptado de Introduction to BPMN, por Stephen A. White, 2004.

2.7 Herramientas utilizadas

Es esta sección se enumeran algunas de las herramientas utilizadas por la organización y que son de importancia para el desarrollo de este proyecto.

2.7.1 Keepass

Keepass (s.f) define esta herramienta como un gestor de contraseñas de código abierto y gratuito. Su forma de funcionamiento consiste en la creación de una base de datos que contendrá todos los usuarios, ambientes y contraseñas y la cual se accede mediante una contraseña maestra. Entre las principales características mencionadas por Keepass (s.f) se encuentran:

- Además de la posibilidad de utilizar la clave maestra, también permite el uso de archivos clave para acceder a la base de datos. Como limitante, se debe llevar el archivo clave consigo cada vez que se desee acceder a las contraseñas registradas en Keepass.
- La herramienta permite combinar ambos métodos de desbloqueo de la base de datos de contraseñas: archivo clave y contraseña maestra.
- Para dispositivos con sistema operativo Windows, permite ser accedido sin necesidad de instalar.
- Keepass no deja ningún rastro en los dispositivos. Esto brinda mayor seguridad ya que no permite que se pueda corromper o acceder por medio de archivos almacenados en los equipos.
- Permite descargar las contraseñas en múltiples formatos. Por ejemplo: HTML, XLM, CSV, entre otros.
- Permite generar contraseñas aleatorias y según especificaciones del usuario, por ejemplo: selección de la cantidad de caracteres, inclusión de símbolos especiales, definir secuencias de caracteres, entre otros.

2.7.2 Confluence

Confluence (s.f) detalla esta herramienta como una plataforma para la gestión organizacional del conocimiento, colaboración en proyectos mediante el desarrollo y publicación de artículos en forma jerárquica. Esta herramienta permite que múltiples usuarios puedan crear artículos,

publicarlos y que el resto de los miembros de la organización puedan accederlos múltiples veces. Entre las principales funciones, Confluence (s.f) destaca las siguientes:

- Ofrece distintas opciones de alojamiento como cloud, data center autogestionado y servidor propio.
- Variabilidad de plantillas que permiten a la organización basarse en estas para la creación de documentos internos.
- Permite la creación de páginas de forma jerárquica, esto para tener mejor visualización de documentos que dependan de otros.
- Permite la creación de espacios, los cuales permiten la división lógica de distintas áreas. Por ejemplo: un espacio para la gestión de conocimiento, un espacio para el registro de información sobre clientes, otros.
- Posibilidad de que distintos colaboradores de la organización actualicen y enriquezcan un mismo documento.

2.7.3 Bizagi Modeler

Según Bizagi (s.f), se puede definir esta herramienta como un software colaborativo que permite la creación de flujos de proceso para ser construidos por múltiples recursos a la vez y de forma intuitiva. Esta herramienta está basada en la notación estándar de modelado de procesos BPMN. Entre los principales beneficios de esta herramienta se encuentran:

- Permite exportar el diagrama realizado en múltiples tipos de documentos como: PDF, JPG, Excel, otros.
- Brinda facilidades que permiten a las organizaciones identificar cuellos de botella en sus procesos, y, por tanto, discutir la forma de atacarlos.
- Construcción y edición colaborativa de procesos mediante la vista web de la herramienta.
- Permite la navegación de extremo a extremo mediante la inclusión de subprocesos dentro de un flujo.
- Posee una biblioteca de procesos como base para la construcción de los procesos de la organización.

- Permite la simulación de procesos mediante la asignación de tiempos, distribuciones estadísticas, recursos, fechas y horarios. Estas simulaciones son de gran importancia ya que posibilitan a las organizaciones medir el esfuerzo humano y financiero necesario para ejecutar un determinado proceso.

3. Marco Metodológico

En este capítulo se detalla la estrategia metodológica que será utilizada para el desarrollo del presente proyecto.

3.1 Tipo de Investigación

Para Hernández et al. (2014) se puede definir una investigación como un conjunto de procesos, los cuales pueden ser sistemáticos, críticos y empíricos, y que suelen aplicarse al estudio de un determinado problema.

Siendo así, Mercado et al (2004) menciona la existencia de dos tipos de investigación: la aplicada y la básica. El tipo de investigación aplicada es definida por Mercado et al (2004) como aquella cuyo principal propósito es aplicar el conocimiento generado a los problemas del sector donde se realice la investigación. Por tanto, se indica que permite la resolución de problemas por medio de prácticas.

En cuanto al tipo de investigación básica, Mercado et al (2004) señalan que esta se encarga de generar conocimiento basado en la investigación, pero tal conocimiento generado nunca se aplicará en entornos prácticos.

Por tanto, y según los tipos de investigación expuestos en esta sección, se determina que la presente investigación es de tipo aplicada, ya que el conocimiento que se genere se aplicará a las actividades cotidianas de la organización.

3.2 Enfoque de investigación

Para Naranjo (2020), los enfoques cualitativo y cuantitativo, en su gran mayoría abarcados por los paradigmas positivista y naturalista, así como el enfoque mixto, el cual se encuentra dentro del paradigma pragmático, están enfocados en el desarrollo metodológico de proyectos e investigaciones de carácter social y en el área de las humanidades. Este tipo de enfoques, como, por ejemplo, el mixto, involucran dificultades asociadas a determinar qué tan cualitativa o qué tan cuantitativa debe ser una determinada investigación, definiciones asociadas a investigadores con alta experiencia y recorrido. Por ello, producto de la no existencia de un enfoque especializado para los proyectos del área informática que facilite la labor de investigadores no tan experimentados, nace el enfoque alternativo.

Según Naranjo (2020), para el enfoque alternativo, perteneciente al paradigma pragmático, basta con probar que la investigación en ejercicio cumple con las dimensiones epistemológica, ontológica y axiológica, además, menciona que este enfoque brinda al investigador la libertad de seleccionar los instrumentos para recuperar información y el diseño de investigación que más se apegue a su proyecto, sin tener que cerrarse a su pertenencia a los enfoques cualitativo, cuantitativo o mixto.

Las dimensiones mencionadas anteriormente deben abarcar lo siguiente:

- Dimensión Epistemológica: Se refiere al papel que asume el investigador hacia su objeto de estudio, ya sea como observador o como un involucrado.
- Dimensión Ontológica: Se demuestra el objeto de estudio por un medio tangible, usualmente una figura que exponga los elementos por estudiar y la relación que existe entre estos.
- Dimensión Axiológica: Rúbrica que permite hacer medibles los objetivos de la investigación según los términos seleccionados, para disminuir conforme sea posible, la subjetividad de las palabras ambiguas denominadas *buzzwords*.

3.2.1 Epistemología

Según Naranjo (2020), el investigador en el área de las investigaciones aplicadas asume un papel de participante de los acontecimientos que rodean su objeto de estudio, por ello, en esta investigación se asume dicha postura.

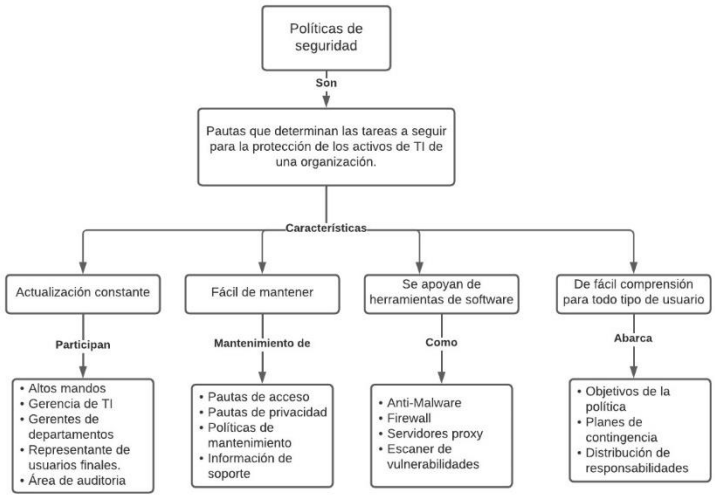
Esta postura está determinada por la necesidad del investigador de conocer la situación actual en la que se encuentra la ejecución de las políticas de seguridad y sus procesos asociados, así como el ambiente organizacional que rodea la aplicación o no aplicación de las políticas. Además, el investigador debe participar de los procesos de actualización y mejora aquellos asociados a dichas políticas de seguridad. Por lo tanto, la información necesaria para el desarrollo de esta investigación se obtiene siendo participante.

3.2.2 Ontología

La Real Academia Española define la Ontología como la "parte de la metafísica que trata del ser en general y de sus propiedades trascendentales" (Real Academia Española, 2021). Siendo así, resulta importante demostrar en esta sección algunas de las propiedades de las políticas de seguridad que determinen su existencia.

Por su parte, se puede determinar la ontología como "la ciencia de lo que es, de los tipos y estructuras de objetos, propiedades, eventos, procesos, y relaciones en cada área de la realidad" (Smith, 2001). Basado en este concepto, en la Ilustración 8. Ontología de las políticas de seguridad, se abarcan detalles de las políticas de seguridad como características y relaciones con el ambiente de las tecnologías de información.

Ilustración 8. Ontología de las políticas de seguridad



Fuente: Adaptado de Diseño e implementación de una política de seguridad, por Néstor D. Duque, 2002

En conclusión, Díaz et al. (2009) señalan que la ontología describe, mediante conceptos y relaciones, la representación de un área de conocimiento en específico; por eso, según la Ilustración 8. Ontología de las políticas de seguridad, se puede validar la ontología de las políticas de seguridad, y, por tanto, la existencia de esta área de conocimiento.

3.2.3 Axiología

Este término, concebido como “teoría de los valores” (Real Academia Española, 2021) define la dimensión axiológica del enfoque alternativo.

En el caso de este proyecto, la dimensión axiológica requiere la medición de los conceptos “Oportunidad de mejora” y “Efectividad”. Estas palabras requieren ser documentadas según las escalas definidas y, tomando como base los datos obtenidos de la aplicación de las actividades correspondientes a cada objetivo.

La oportunidad de mejora será evaluada con la escala definida en la Tabla 6. Rubros de evaluación de oportunidad de mejora. Cada uno de estos rubros es una primera propuesta para la

medición del término “Oportunidad de mejora”, dado que en la literatura no existe un estándar o marco de referencia que brinde rubros por aplicar.

Cada uno de los rubros propuestos para oportunidad de mejora fue seleccionado por las siguientes razones:

- Documentación existente: La importancia de la documentación que respalde una política radica en la posibilidad que tiene esta de ser replicada como conocimiento al resto de la organización. Una política no documentada puede provocar que se generen ambigüedades en su uso, según el usuario que la aplique. Por tanto, una política sin documentar realmente suma porcentaje para ser identificada como una política con oportunidad de mejora. Este rubro representa un 50% del total, debido a que la falta de documentación, sin duda alguna, es una de las principales razones de la gestión desarticulada de las políticas de seguridad en la organización.
- Aplicación en tribus: Como ya se mencionó, la organización trabaja a partir de subgrupos denominados *tribus*. Como las políticas son de aplicación organizacional, es necesario conocer el nivel de arraigo que tiene una política en la organización, y este nivel de arraigo se debe interpretar como el número de tribus que aplican la política en sus funciones diarias. Este rubro representa un 35% del total, dado que ayuda a medir qué tan reconocida puede ser una política para los miembros pertenecientes a las tribus de la organización.
- Aprobaciones necesarias: El problema principal que se pretende abordar en esta investigación es la gestión desarticulada de la seguridad, por tanto, es necesario controlar el nivel de aprobaciones eventual de las políticas; esto con la finalidad de evitar que muten dependiendo de los colaboradores o roles que realicen aprobaciones relacionadas con las políticas. Este rubro cuenta con un porcentaje de 15, pues, aunque es importante, no presenta el mismo peso que el resto de los rubros pueden tener para la gestión de las políticas.

Tabla 6. Rubros de evaluación de oportunidad de mejora

Oportunidades de mejora				
Rubro	Descripción del rubro	Valor	Opciones	
Documentación existente	La política cuenta o no con documentación que la respalde.	50%	No cuenta con documentación: 50%	Cuenta con documentación: 10%
Aprobaciones necesarias	Número de aprobaciones necesarias para la culminación del proceso.	15%	Requiere más de dos aprobaciones: 15%	Requiere dos o menos aprobaciones: 5%
Aplicación en tribus	Número de tribus que aplican la política.	35%	Se aplica en tres tribus o menos: 35%	Se aplica en más de tres tribus: 5%

Fuente: Elaboración propia, 2022.

Según la escala contenida en la Tabla 6. Rubros de evaluación de oportunidad de mejora, mientras mayor sea el porcentaje obtenido, mayor será considerada la política como candidata a oportunidad de mejora. Se considera que un 70% o más, será considerado como una política con oportunidad de mejora alta; 50% o más, será tomado como una oportunidad de mejora media; mientras que un porcentaje menor a 50% será tomado como una política con oportunidad de mejora baja. En la Tabla 7. Resumen porcentajes oportunidad de mejora, se muestran los rangos de porcentajes obtenidos con su respectivo significado.

Tabla 7. Resumen porcentajes oportunidad de mejora

Porcentaje obtenido	Significado
Entre 70% y %100	Oportunidad de mejora alta
Entre 50% y 69%	Oportunidad de mejora media
Entre 20% y 49%	Oportunidad de mejora baja

Fuente: Elaboración propia, 2022.

La efectividad será evaluada según la escala expuesta en la Tabla 8. Rubros de evaluación de efectividad. Se tomaron en cuenta los siguientes rubros:

- Documentación existente: Se debe considerar como parte fundamental de las políticas de seguridad la documentación existente sobre estas. Dicha documentación permite a las organizaciones establecer estrategias de difusión y comunicación de las buenas prácticas organizacionales para resguardar la seguridad. Este rubro representa un 50% del total, debido a que la documentación es una de las principales herramientas para gestionar de forma articulada la seguridad; al ser la misma documentación para toda la organización, las tribus existentes se apegarán al mismo estándar.
- Número de actores: El total de colaboradores involucrados en la ejecución de una política de seguridad es de gran importancia, debido a que, al tratarse de aspectos de seguridad de la información, se debe tener una ejecución rápida y poco burocrática. Este rubro representa un 25% del total del porcentaje y se iguala al rubro “Aprobaciones necesarias”, debido a que ambos están estrictamente relacionados.

- Aprobaciones necesarias: Como se mencionó anteriormente, para mantener la integridad y buen control sobre una política de seguridad es necesario que las aprobaciones involucradas en las políticas sean llevadas a cabo por un mismo rol, y que este rol sea el mismo, independientemente de la tribu o colaborador que aplique una determinada política. Se determina que una política de seguridad de la información será efectiva si cuenta con un número reducido de aprobaciones. Este rubro representa un 25% del porcentaje total, ya que, como se indicó anteriormente, está enlazado al rubro "Número de actores", que también tiene el mismo porcentaje.

Tabla 8. Rubros de evaluación de efectividad

Efectividad				
Rubro	Descripción del rubro	Valor	Opciones:	
Número de actores	Número de actores involucrados en la política	25%	Las personas involucradas en la política son mas de tres: 5%	Las personas involucradas en la política son tres o menos: 25%
Documentación existente	Existencia de documentación que soporte la política.	50%	La política no cuenta con documentación: 5%	La política cuenta con documentación: 50%
Aprobaciones necesarias	Mayor número de aprobaciones necesarias para la culminación de un proceso perteneciente a la política.	25%	Requiere más de dos aprobaciones: 5%	Requiere dos o menos aprobaciones: 25%

Fuente: Elaboración propia, 2022.

Según la Tabla 8. Rubros de evaluación de efectividad, mientras mayor sea el porcentaje obtenido por la política al ser evaluada, mayor será la efectividad de esta, por tanto, se considera que un porcentaje mayor a 75% será considerado como una política efectiva. Por otra parte, un porcentaje menor a 75% será considerado como una política carente de efectividad. En la Tabla 9. Resumen porcentajes efectividad, se muestra el significado de los rubros de acuerdo con la suma de porcentajes obtenidos.

Tabla 9. Resumen porcentajes efectividad

Porcentaje obtenido	Significado
Entre 75% y %100	Política efectiva
Entre 15% y 74%	Política carente de efectividad

Fuente: Elaboración propia, 2022.

Cada uno de los rubros y porcentajes asociados a la axiología fueron validados tanto por una persona interna a la organización como por un experto; esto, según lo expresado en el Apéndice K - Minuta EM 05 – 1606 y por medio de comunicaciones personales.

Según lo indicado por el interesado de la organización, “Cada una de las métricas utilizadas y los rubros indicados se adapta de gran manera tanto a las políticas utilizadas como a la situación actual de Xumtech” (H.Brenes, comunicación personal, 16 de junio de 2022).

3.3 Diseño de la Investigación

Esta sección tiene como objetivo mostrar los distintos tipos de investigación existentes, así como seleccionar el que más se adapte a este proyecto.

Según lo determinado por Naranjo (2020), una de las principales ventajas del enfoque alternativo es que permite seleccionar el diseño de investigación que más se adapte al proyecto; esto, tomando en cuenta los diseños de investigación del enfoque cualitativo y cuantitativo.

Por tanto, Hernández et al. (2014) define, por ejemplo, para la investigación de tipo cualitativa diseños como:

- Teoría fundamentada: Mayormente utilizada cuando no se tienen teorías por aplicar.
- Diseño etnográfico: Utilizado para el estudio de sistemas sociales.
- Diseño narrativo: Describe que un conjunto detallado de historias colabora en la comprensión de un problema.

- Diseño fenomenológico: Estudia las distintas perspectivas de un determinado fenómeno.
- Diseño de investigación/acción: Su aplicación está determinada por la resolución y mejora de una problemática que pretende establecer un cambio sobre el objeto de estudio.

En el caso de este proyecto, se cumple con el diseño de investigación/acción, ya que se pretende establecer un cambio sobre la forma en que la organización gestiona y promueve el uso articulado de las políticas de seguridad y sus procesos asociados.

Para el diseño de investigación/acción, Hernández et al. (2014) mencionan la existencia de los siguientes ciclos que lo respaldan:

- Identificar la problemática: Ejecución de las tareas necesarias para asegurar la correcta identificación del problema raíz.
- Elaborar un plan: Se abarca con la recolección de datos para generar el plan y la etapa de desarrollo del plan.
- Implementar y evaluar el plan: Se encarga de poner en marcha el plan, además, involucra una nueva etapa de recolección de datos para tener los insumos suficientes para evaluar el plan implementado.
- Retroalimentación: El objetivo de este ciclo es ajustar el plan según los hallazgos realizados.

3.4 Fuentes de Investigación

Para lograr un desarrollo de la investigación acotado y a la medida de la situación actual de la organización, es de vital importancia contar con fuentes de información que permitan conocer lo que se tiene actualmente y a lo que se desea llegar. Para una mejor comprensión de su naturaleza, estas fuentes de información serán separadas en dos grupos: fuentes de información primarias y fuentes de información secundarias.

3.4.1 Fuentes de información primarias

Para Hernández et al. (2014), las fuentes de información primarias corresponden a aquellas que contienen información catalogada como no alterada u original, lo cual quiere decir que son obtenidas de revistas científicas, informes técnicos, libros, entre otros.

Para el desarrollo de este proyecto se consideran fuentes de información primarias los siguientes:

- Artículos científicos relacionados con el desarrollo e implementación de políticas de seguridad.
- Manuales de la notación de administración de procesos de negocio, necesarios para la diagramación *As-is* y *To-be* de los procesos asociados a las políticas, así como apoyo en la evaluación de los procesos y la simulación de estos.
- Artículos científicos con información referente a la metodología, y por tanto, al enfoque de investigación alternativo.
- Marcos de referencia sobre las mejores prácticas en el área de la seguridad informática, como por ejemplo COBIT 5, Centro de Seguridad en Internet *(CIS*, por sus siglas en inglés) y el Instituto Nacional de Estándares y Tecnología (*NIST*, por sus siglas en inglés).
- Documentación interna de respaldo de los procesos de seguridad asociados a las políticas.

3.4.2 Fuentes de información secundaria

Por su parte, las fuentes secundarias son definidas por Hernández et al. (2014) como la recopilación de información de forma ordenada, a partir de datos obtenidos de fuentes primarias.

Dentro de las fuentes secundarias catalogadas como importantes para el desarrollo de este proyecto, se encuentran:

- Documentos web relacionados con conceptos básicos de la gestión metodológica y conceptual del proyecto; esto con fines laborales y académicos.
- Repositorios de tesis y trabajos de graduación relacionados con la gestión de políticas dentro de una organización.
- Repositorios de tesis y trabajos de graduación de la carrera de Administración de Tecnología de información (ATI); esto como guía para la estructura de documento, formato y abordaje de los distintos capítulos.

3.5 Sujetos de Investigación

Los sujetos de investigación son aquellos involucrados que se considera tienen amplio conocimiento sobre los procesos por investigar. Son actores importantes en la ejecución diaria de los procesos relacionados con la investigación.

La Tabla 10. Sujetos de investigación, da detalles sobre las responsabilidades de cada sujeto de investigación, así como porqué es importante para esta.

Tabla 10. Sujetos de investigación

Rol del sujeto	Caracterización del sujeto	Justificación
Dueño de producto (PO)	Líder de una determinada Tribu. Dueño de producto del proyecto o proyectos a cargo de la Tribu. Gestiona el diseño de implementación, cronograma y alcance de las iniciativas a cargo de la Tribu.	Es quien propone y valida los procesos relacionados a seguridad que más se adapten al cliente, y por ende, a la Tribu. Además, promueve el desarrollo de las metodologías de trabajo ágil en la totalidad de su Tribu. Punto más cercano entre la Tribu y los altos mandos.
Líder Técnico (LT)	Se encarga de la gestión del equipo asignado a la Tribu, esto con la finalidad de cumplir con lo estipulado en alcance y cronograma. Gestiona la documentación relacionada a los requerimientos del cliente.	Es el responsable de la ejecución de los procesos relacionados a seguridad por parte de los miembros de la Tribu. Asegura el cumplimiento de los procesos que maantengan el bienestar del trabajo de la Tribu.
Consultor	Encargado de labores de seguimiento y construcción de las implementaciones. Además, se encarga de la gestión de requerimientos del cliente mediante sesiones y gestión documental.	En sus labores cotidianas debe aplicar los procesos de seguridad necesarios para conservar la integridad de la información de la Tribu y del cliente.

Fuente: Elaboración propia, 2022.

3.6 Variables de la Investigación

En esta sección se definen las variables de investigación asociadas a este proyecto. Estas tienen como principal función medir y validar el cumplimiento de los objetivos específicos planteados.

Como se mencionó anteriormente, las variables están definidas por cada objetivo específico; por ello, se definió una tabla de información para cada uno de los tres objetivos del proyecto.

En la Tabla 11. Variables de investigación del primer objetivo específico, se especifican las variables para el primer objetivo.

Tabla 11. Variables de investigación del primer objetivo específico

Objetivo específico:	Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.		
Variable	Tipo	Indicadores	Detalle
Procesos actuales	Independiente	Cantidad de procesos existentes	Los procesos actuales son de vital importancia ya que permiten conocer el nivel de madurez en que se encuentra la organización, así como los vacíos eventuales en relación con procesos de seguridad faltantes.
Oportunidades de mejora	Dependiente	Nivel de la oportunidad de mejora	Determina las debilidades que deben ser actualizadas tomando como insumos las mejores prácticas del mercado.

Fuente: Elaboración propia, 2022.

En la Tabla 12. Variables de investigación del segundo objetivo Se detallan las variables tomadas para el segundo objetivo específico.

Tabla 12. Variables de investigación del segundo objetivo

Objetivo específico:	Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria.		
Variable	Tipo	Indicadores	Detalle
Políticas de seguridad	Independiente	Cantidad de políticas de seguridad	Políticas de seguridad para proponer a la organización.
Procesos asociados a las políticas de seguridad	Dependiente	Cantidad de procesos asociados a las políticas	Procesos que estarán asociados a las políticas propuestas.

Fuente: Elaboración propia, 2022.

En la Tabla 13. Variables de investigación del tercer objetivo, se muestran las variables de investigación para el tercer objetivo.

Tabla 13. Variables de investigación del tercer objetivo

Objetivo específico:	Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis financiero para la validación de la efectividad de las mejoras propuestas.		
Variable	Tipo	Indicadores	Detalle
Procesos propuestos	Independiente	Cantidad de procesos propuestos	Corresponde a los procesos propuestos para cubrir las políticas de seguridad identificadas en la situación actual.
Efectividad de los procesos propuestas	Dependiente	Nivel de efectividad de las mejoras propuestas	Necesario para medir la efectividad de los procesos propuestos para la organización.

Fuente: Elaboración propia, 2022.

3.7 Instrumentos de Investigación

Hernández et al. (2014) definen los instrumentos de investigación como aquellas herramientas que permiten obtener la información requerida para el proceso investigativo, así como construir el conocimiento acerca de lo que se investiga.

En esta sección, se brinda detalle sobre los instrumentos de investigación utilizados en este proyecto.

3.7.1 Cuestionario

Para García (2003) un cuestionario corresponde a un procedimiento clásico de las ciencias sociales que permite obtener información y registro de datos. Además, se detalla como un conjunto de preguntas ordenadas sistemáticamente para obtener la información que interesa a la investigación.

Su principal objetivo es, tomando como base las variables de estudio, obtener información de la población con la que se trabaja en el proyecto.

Becerra (2012) señala que dentro de un cuestionario existen distintos tipos de preguntas para obtener información. Estos tipos de preguntas son:

- Cerradas: Pregunta delimitada por cierto número de respuestas, por lo que el sujeto solo puede seleccionar una de las respuestas brindadas.
- Abiertas: No delimitan la respuesta del encuestado a valores fijos. El sujeto de estudio tiene libertad de ingresar la respuesta y cantidad de información a discreción.
- Mixtas: Se refiera a un cuestionario formado con preguntas de temática abierta y temática cerrada.

Para obtener información relacionada con este proyecto se optó por la creación de una encuesta de tipo mixta, de la cuál queda evidencia en Apéndice B - Encuesta a líderes técnicos y consultores. Esta encuesta fue aplicada a los sujetos de estudio líder técnico y consultor.

3.7.2 Entrevista

Según García et al. (s.f) se puede determinar una entrevista como el instrumento con el cuál el investigador pretende, de forma personal y extendida, obtener información relevante sobre su objeto de estudio.

Como parte del anterior concepto, García et al. (s.f) señalan que una entrevista debe cumplir las siguientes características:

- Recopila información tanto subjetiva como objetiva.
- Debe contener, como mínimo, un referente, un código, un mensaje y un medio por el cual se transmita.
- Debe utilizar un sistema de comunicación interpersonal.
- El entrevistador es el encargado de guiar la conversación de tal manera que recopile la información que necesite.

Además, Hernández et al. (2014) señalan que existen distintos tipos de entrevistas, las cuáles se exponen a continuación.

- Estructuradas: Se planifican previamente las preguntas por realizar con un orden secuencial. El entrevistado solo podrá emitir comentarios relacionados con la pregunta que se realice.
- Semiestructuradas: El entrevistador elabora un guion sobre las preguntas que desea realizar. Al ser abiertas, el entrevistado puede emitir puntos de vista que se salgan de la estructura de la pregunta y que agreguen valor a la información.
- Abiertas: No se realiza ningún tipo de guion de preguntas. Durante la conversación con el entrevistado se recupera la información de forma espontánea.

Para la realización de este proyecto se aplicó un total de tres entrevistas de tipo abierto al sujeto de estudio dueño de producto. Para las entrevistas *(insertar minutas)* se utilizaron como base los temas expuestos en Apéndice A - Temas entrevista .

3.7.3 Revisión documental

Para Hernández et al. (2014) la revisión documental consiste en consultar información física o digital con la que cuente la organización y/o el objeto de estudio. Además, menciona que es uno de los instrumentos para recopilar información más sencillos, debido a su alta disponibilidad y poca dependencia de otras personas. Como punto crítico, se menciona que alguna información puede estar restringida por contener datos considerados como sensibles.

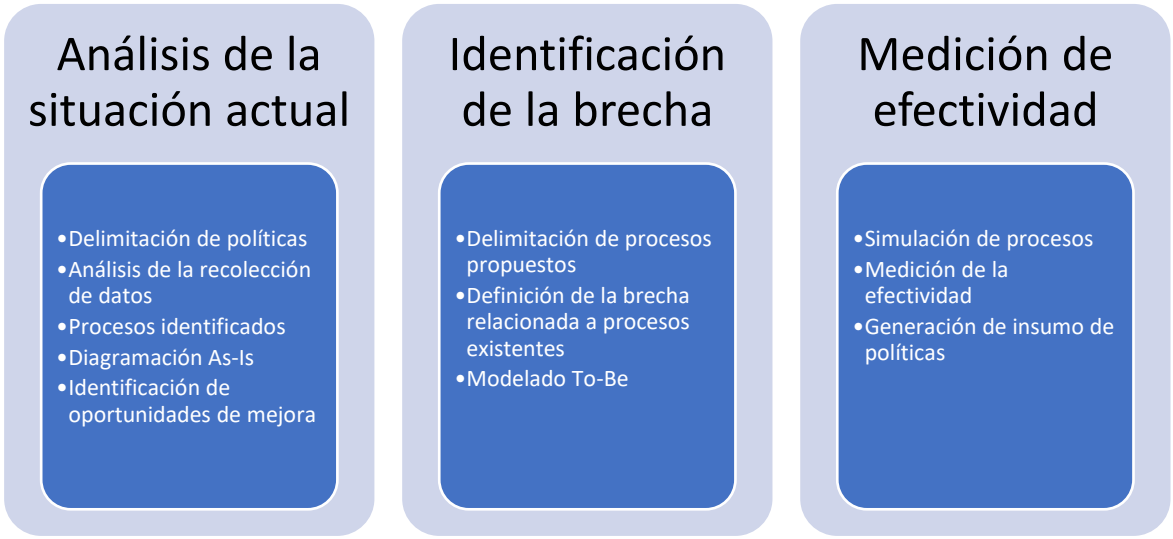
En este proyecto se realizó la revisión documental sobre los artículos relacionados con los procesos de seguridad con los cuales cuenta la organización. Para la evidencia relacionada a la revisión documental, esta se registra en la plantilla expuesta en Apéndice C – Plantilla de Revisión documental.

3.8 Procedimiento metodológico de la Investigación

Para Hernández et al. (2014) la investigación se define como la elaboración de una propuesta final basada en un proceso que inicia con la recolección de información sobre el objeto de estudio.

En la Ilustración 9. Procedimiento metodológico de la investigación, se evidencia cómo se realizó la metodología de investigación separada por fases, así como las actividades que cada una de estas implicó. A continuación, se detallan las actividades mencionadas.

Ilustración 9. Procedimiento metodológico de la investigación



Fuente: Elaboración propia, 2022.

3.8.1 Fase 1. Análisis de la situación actual

Al tratarse de la primera fase de esta metodología y tomando en cuenta el diseño de la investigación, se incluyen tareas relacionadas con la recuperación de información sobre la situación de la empresa, así como la delimitación de las políticas de seguridad por abarcar. Entre las actividades involucradas se encuentran:

- Delimitación de políticas

Esta actividad consiste en seleccionar, en conjunto con la organización, las políticas de seguridad que participan de esta investigación. Previo al proceso de selección de las políticas, se

realizó una revisión de los documentos de la empresa, así como de marcos de referencia de la industria; esto con la finalidad de elaborar una lista de políticas propuestas y facilitar la selección final.

- Análisis de la recolección de datos

Según los instrumentos de investigación expuestos en la metodología y los distintos sujetos de investigación seleccionados, esta actividad consiste en la aplicación de los instrumentos sobre los sujetos determinados, con la finalidad de obtener la información sobre la situación actual de la empresa, la cual servirá de insumo para siguientes fases y actividades.

Esta actividad conlleva la recopilación de información que, al ser utilizada en otras fases, determinará los pasos por seguir sobre las políticas y procesos existentes, así como las políticas y procesos por proponer.

- Diagramación As-Is

Esta actividad utiliza como insumo la información obtenida de la aplicación de los instrumentos de investigación. Mediante el uso de la metodología BPMN, se diagraman los procesos asociados a las políticas de seguridad existentes en la organización. Los diagramas resultantes serán los insumos necesarios para las propuestas y actualizaciones que se realizan en futuras fases y actividades.

- Identificación de oportunidades de mejora

Según lo definido en Tabla 6. Rubros de evaluación de oportunidad de mejora de la dimensión axiológica del enfoque alternativo, en esta tarea se toman como entradas los diagramas generados en metodología BPMN, con el objetivo de identificar el puntaje obtenido basado en los rubros que determinan la oportunidad de mejora de un determinado proceso. Esta evaluación determinará si, según el contexto de la organización, estos procesos requieren ser actualizados de acuerdo con la brecha identificada.

3.8.2 Fase 2. Identificación de la brecha

Esta fase tiene como objetivo definir la brecha existente entre los procesos actuales de la organización y lo dictado por los marcos de referencia de la industria. Entre la identificación de la brecha se abarca la actualización a políticas y procesos ya existentes, así como la propuesta de nuevas políticas y procesos que se consideren necesarios para la operación cotidiana de la empresa.

Entre las actividades más importantes también se contempla la diagramación de los nuevos procesos y la actualización de los existentes, según la brecha identificada. Entre las actividades se encuentra:

- Delimitación de procesos propuestos

Según la revisión documental sobre los marcos de referencia y los resultados obtenidos de la identificación de las oportunidades de mejora sobre los procesos existentes, esta tarea consiste en listar los procesos que se proponen como nuevos y que formarán parte de las políticas seleccionadas.

Esta delimitación será coordinada con la organización, ya que es de vital importancia contar con el criterio de la parte interesada.

- Definición de la brecha relacionada a procesos existentes

Basado en la diagramación As–Is y en el análisis documental de los marcos de referencia seleccionados, en esta tarea se identifican las actualizaciones a las cuales serán sometidos los procesos identificados; esto según las buenas prácticas indicadas por los marcos de referencia consultados. Estas actualizaciones serán insumo de las posteriores fases y actividades.

- Modelado To-Be

Mediante la metodología BPMN, esta tarea tiene como objetivo modelar las actualizaciones a las que serán sometidos los procesos existentes, así como la secuencia de pasos que tendrán los nuevos procesos propuestos.

Esta diagramación será el principal insumo de la Fase 3, la cual involucra mediciones que determinarán la efectividad de las propuestas realizadas.

3.8.3 Fase 3. Medición de efectividad

Tal y como su título lo indica, esta fase involucra tareas que determinarán a la organización los resultados que se espera obtener de los procesos y políticas de seguridad actualizados y los propuestos.

Esta fase utiliza como principales insumos las brechas identificadas en la anterior fase, así como la diagramación To-be, resultante de los análisis documentales. Entre las tareas que abarca esta fase se encuentra:

- Simulación de procesos

Brinda a la organización información relacionada con los tiempos involucrados para la aplicación cotidiana de los procesos actualizados y los propuestos. Este insumo es de gran importancia para la empresa, ya que actualmente no se cuenta con mediciones de este tipo, lo cual permite la futura evaluación de tiempo total y costos invertidos en la aplicación y gestión de las políticas de seguridad de la información.

- Medición de la efectividad

Según lo definido en Tabla 8. Rubros de evaluación de efectividad, esta actividad conlleva la aplicación de los rubros definidos para la evaluación de la efectividad en los procesos propuestos y actualizados. Como base, esta actividad toma la diagramación To-Be realizada, y sobre estos insumos se aplican los rubros detallados en la tabla citada.

Esta actividad brinda como resultado la efectividad de los determinados procesos, tomando en cuenta los rubros definidos según recomendación de los expertos.

- Análisis financiero

Consta de la aplicación de indicadores financieros que demuestren con cifras el costo de implementar los procesos propuestos asociados a las políticas. Esto brinda información importante a la organización, relacionada con los costos que involucra proteger la información.

- Generación de insumo de políticas

Se refiere a la creación de un insumo que funcione como documentación interna para la organización y que dé una guía clara sobre las políticas de seguridad propuestas y los procesos que estas abarcan.

3.9 Matriz de cobertura de las variables

En la Tabla 14. Cobertura de las variables, se presentan los instrumentos de investigación que permiten abarcar la información necesaria para el correcto desarrollo de las variables de investigación.

Tabla 14. Cobertura de las variables

Variables	Entrevista	Cuestionario	Revisión documental
Procesos actuales			X
Oportunidades de mejora	X	X	X
Políticas de seguridad		X	X
Procesos asociados a las políticas de seguridad		X	X
Procesos propuestos			X
Efectividad de los procesos propuestos		X	X

Fuente: Elaboración propia, 2022.

3.10 Matriz de trazabilidad del procedimiento metodológico de la investigación

Los objetivos específicos definidos para este proyecto se detallan a continuación:

- OB1: Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.
- OB2: Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria.
- OB3: Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis financiero para la validación de la efectividad de las mejoras propuestas.

En la Tabla 15. Trazabilidad del procedimiento metodológico, se brinda un resumen de la relación entre los objetivos planteados y los distintos capítulos de este proyecto.

Tabla 15. Trazabilidad del procedimiento metodológico

Objetivo	Marco conceptual	Marco metodológico	Análisis de resultados	Propuesta de solución	Conclusiones	Recomendaciones
OB1	○ 2.5 ○ 2.6	○ 3.8.1 ○ 3.2.3	○ 4.1 ○ 4.3 ○ 4.4 ○ 4.5	No aplica	Conclusiones: Objetivo 1	Recomendaciones: Objetivo 1
OB2	○ 2.5 ○ 2.1 ○ 2.6 ○ 2.2	○ 3.8.2	No aplica	○ 5.1 ○ 5.2	Conclusiones: Objetivo 2	Recomendaciones: Objetivo 2
OB3	○ 2.5 ○ 2.3	○ 3.8.3 ○ 3.2.3	No aplica	○ 5.3 ○ 5.4	Conclusiones: Objetivo 3	Recomendaciones: Objetivo 3

Fuente: Elaboración propia, 2022.

3.11 Tabla resumen del procedimiento metodológico de la Investigación

En esta sección se muestra un resumen que abarca las definiciones realizadas en este capítulo y que tienen como objetivo asegurar el cumplimiento de las variables de investigación. En la Tabla 16. Operalización de las variables, se muestra el detalle del resumen en el cual se hizo énfasis anteriormente.

Tabla 16. Operalización de las variables

Fase de la investigación	Objetivo que se logra en la fase	Variables de investigación	Instrumentos de investigación	Sujetos de investigación
Análisis de la situación actual	Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.	Procesos actuales, oportunidades de mejora	Entrevista, cuestionario, revisión documental	Dueño de producto, Líder técnico, Consultor
Identificación de la brecha	Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria	Políticas de seguridad, Procesos asociados a las políticas de seguridad	Entrevista, revisión documental	Dueño de producto
Medición de efectividad	Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis costo beneficio para la validación de la efectividad de las mejoras propuestas.	Procesos propuestos, Efectividad de los procesos propuestos	Entrevista, revisión documental	Dueño de producto

Fuente: Elaboración propia, 2022.

4 Análisis de Resultados

Este capítulo tiene como propósito describir los resultados obtenidos de la aplicación de los instrumentos de investigación descritos en la sección 3.4 Fuentes de Investigación. Así mismo, en esta sección se llevan a cabo las tareas necesarias para la culminación de la Primera Fase de este proyecto, descrita en 3.8.1 Fase 1. Análisis de la situación actual.

4.1 Delimitación de políticas

En este apartado se definen las políticas por abarcar en este proyecto, las cuales se propusieron y seleccionaron mediante la utilización de la entrevista como instrumento de investigación, y según lo abarcado en la Apéndice F – Minuta EM 02 – 0504 .

Para el proceso de selección, primeramente, se realizó una propuesta a la contraparte de la organización. Para dicha propuesta se tomó como base lo expuesto en el marco de referencia descrito en 2.1.1 Controles CIS.

Por tanto, y tomando como base lo anteriormente mencionado, se propusieron las políticas que se presentan en Tabla 17. Políticas propuestas. Estas fueron propuestas con base en los controles CIS pertenecientes al “Grupo de implementación 1” detallado en 2.1 CIS, de los cuales se tuvo la posibilidad de evaluar los que más se adaptan a la organización.

Tabla 17. Políticas propuestas

Control CIS	Nombre de Control CIS	Nombre de política propuesta
8	Defensa contra software malicioso	Gestión de antivirus
4	Control y uso de privilegios administrativos	Gestión de contraseñas basado en herramienta Keepass
13	Protección de datos	Guía de seguridad para nuevos empleados

Fuente: Elaboración propia, 2022.

Según las políticas propuestas y las necesidades señaladas por la organización, se planteó cambiar una de las políticas por otra expuesta por la contraparte de la organización, esto dada una necesidad existente relacionada con la movilización de la empresa a la modalidad de zonas

francas. Por tanto, en la entrevista ejemplificada en el Apéndice F – Minuta EM 02 – 0504, se tomaron como políticas definitivas las detalladas en la Tabla 18. Políticas seleccionadas. La decisión final sobre las políticas estuvo apegada al "Grupo de implementación 1" de los controles CIS, descritos en 2.1 CIS.

Tabla 18. Políticas seleccionadas

Control CIS	Nombre de Control CIS	Nombre de política propuesta
8	Defensa contra software malicioso	Defensa contra software malicioso
4	Control y uso de privilegios administrativos	Control y uso de privilegios administrativos
2	Inventario y control de los activos de software	Inventario y control de los activos de software

Fuente: Elaboración propia, 2022.

4.2 Análisis de la recolección de datos

Para recolectar la información que funciona como principal insumo de este proyecto, y según lo definido en 3.7 Instrumentos de Investigación, en esta sección se muestra el análisis de los resultados de la aplicación del instrumento de investigación definido como *encuesta*. Los datos utilizados en cada una de las siguientes secciones se muestran con mayor detalle en Apéndice J – Conglomerado de datos recopilados de encuesta.

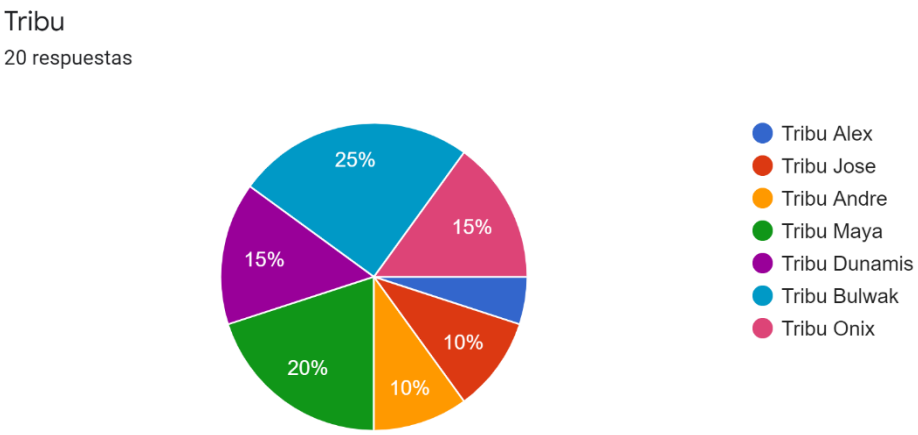
4.2.1 Información general

Como primer punto, es de vital importancia tener clara la forma de trabajo de la empresa Xumtech, la cual se detalla en 1.2.1 Descripción de la organización, que a su vez se vale de los roles expuestos en la Tabla 1. Equipo de trabajo. Una vez claros la forma de trabajo y los roles de la organización, se definen los resultados obtenidos de la aplicación de los instrumentos de investigación.

Para un correcto desarrollo del proyecto, es necesario que los sujetos de estudio estén involucrados en todas las tribus de la organización; esto para tener un panorama más amplio de la forma en la cual se trabajan los temas por investigar. Por tanto, en la Ilustración 10. Tribus de

la organización, se muestra la distribución porcentual del total de participaciones del instrumento de investigación. Es decir, se deja en evidencia que existen siete tribus en la organización. Respecto a las entrevistas abiertas detalladas en Apéndice D – Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804 ambos colaboradores pertenecen a la denominada “Tribu Maya”.

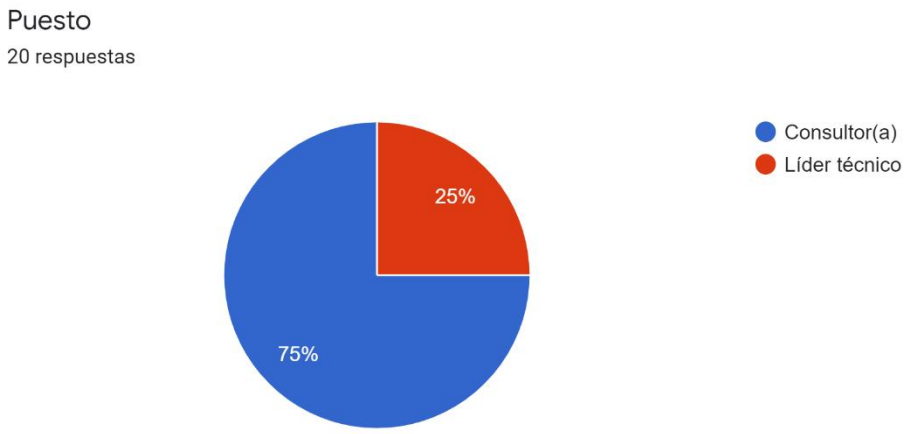
Ilustración 10. Tribus de la organización



Fuente: Elaboración propia, 2022.

En cuanto a los roles participantes de los instrumentos de investigación, en la Ilustración 11. Roles participantes de encuesta se muestra el porcentaje de participación de los roles. Para el instrumento entrevista abierta, detallado en Apéndice D – Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804, el rol utilizado fue *dueño de producto.*

Ilustración 11. Roles participantes de encuesta



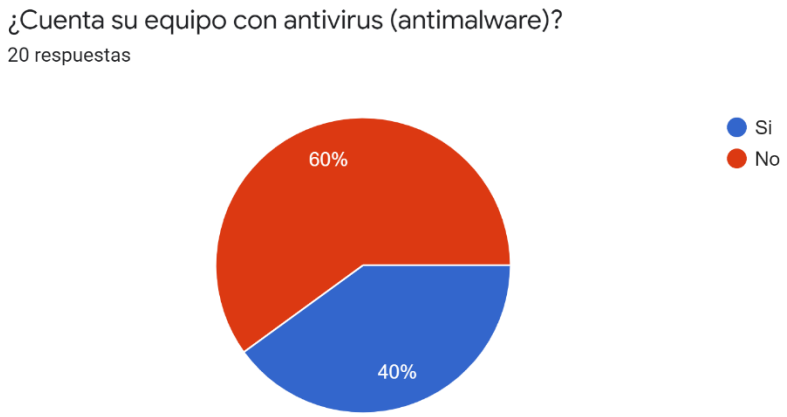
Fuente: Elaboración propia, 2022.

4.2.2 Defensa contra software malicioso

En esta sección se brindan detalles sobre el análisis de la información obtenida de los instrumentos de investigación, en específico, para la política propuesta "Defensa contra software malicioso".

Como primer punto, se consultó a los colaboradores si el equipo cuenta con un programa antivirus instalado; se obtuvieron los resultados expuestos en la Ilustración 12. Presencia de antivirus en equipos.

Ilustración 12. Presencia de antivirus en equipos



Fuente: Elaboración propia, 2022.

Según lo observado en Ilustración 12. Presencia de antivirus en equipos se determina que un 60% de los colaboradores no cuentan con un programa antivirus en su equipo, mientras que un 40% sí lo tienen. Por tanto, se determina que, para ser una empresa de servicios, un porcentaje muy alto de colaboradores no cuentan con un programa antivirus; eso pone en riesgo la información tanto interna como de los clientes. En la Tabla 19. Resumen presencia de antivirus en equipos, se muestra un resumen de los datos obtenidos.

Tabla 19. Resumen presencia de antivirus en equipos

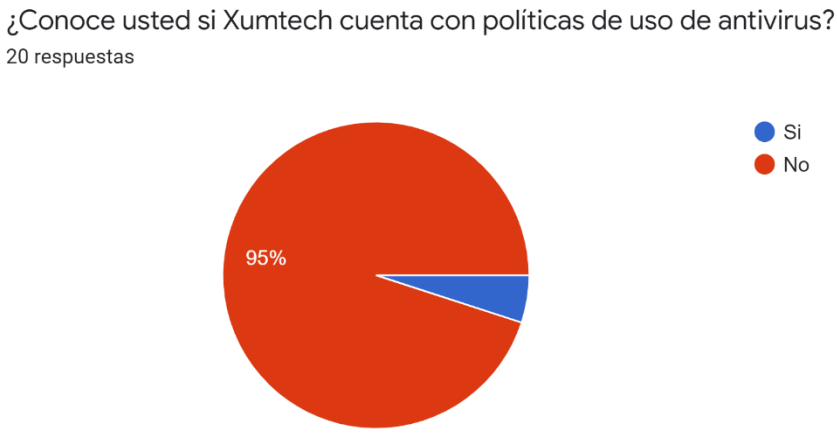
Respuesta	Porcentaje	Total de colaboradores
Sí	40%	8
No	60%	12
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Relacionado con el tema de conocimiento de los colaboradores sobre la existencia de políticas de seguridad relacionadas con el uso de antivirus, se obtuvo como resultado que un 95%

de los colaboradores participantes del instrumento de investigación no tienen conocimiento de si Xumtech cuenta con políticas de uso de antivirus, mientras que un 5% indicó que sí lo saben. Esto se ve ejemplificado en la Ilustración 13. Existencia de política de uso de antivirus.

Ilustración 13. Existencia de política de uso de antivirus



Fuente: Elaboración propia, 2022.

En la Tabla 20. Resumen existencia de política de uso de antivirus, se evidencia que la mayoría de los colaboradores encestados no tiene conocimiento sobre la posición de la organización en cuanto a la gestión de antivirus.

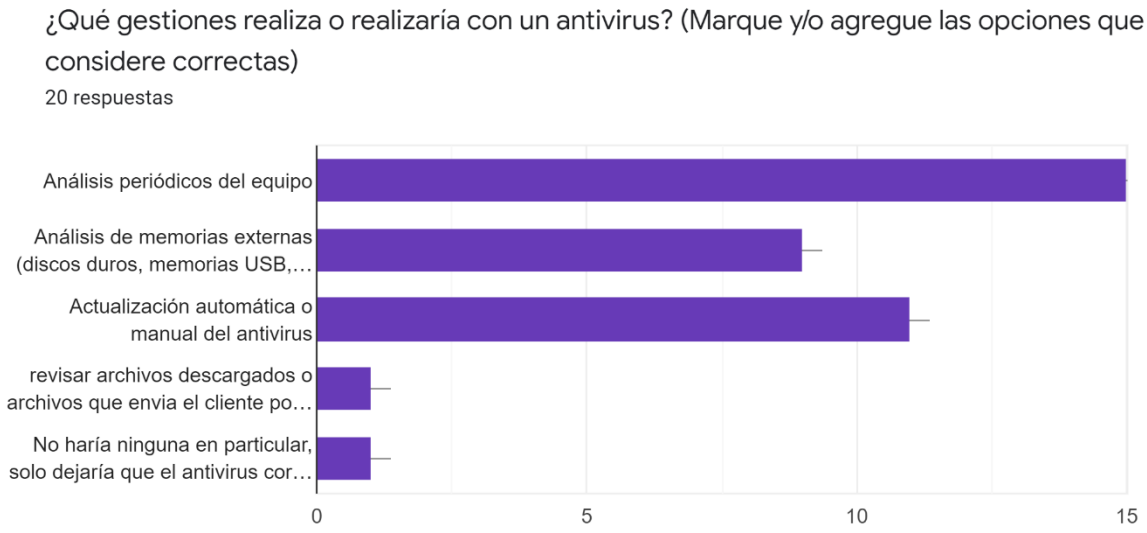
Tabla 20. Resumen existencia de política de uso de antivirus

Respuesta	Porcentaje	Total de colaboradores
Sí	5%	19
No	95%	1
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Además de lo ya mencionado, se consultó a los colaboradores sobre los procesos que harían o realizan con un antivirus, tal y como se muestra en Ilustración 14. Procesos asociados a gestión de antivirus.

Ilustración 14. Procesos asociados a gestión de antivirus



Fuente: Elaboración propia, 2022.

En la Tabla 21. Resumen procesos asociados a gestión de antivirus, se muestra un resumen de los procesos que los colaboradores consideran como importantes, según el uso de un programa antivirus, además, en dicha tabla se muestra el porcentaje y número de colaboradores que apoyan dichos procesos.

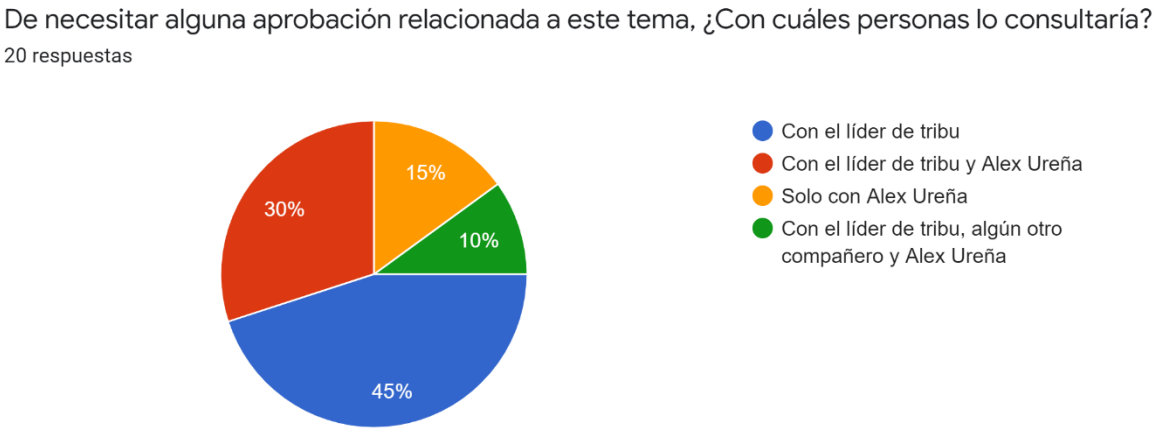
Tabla 21. Resumen procesos asociados a gestión de antivirus

Respuesta	Porcentaje	Total de colaboradores
Análisis periódicos de los equipos	75%	15
Análisis de memorias externas	45%	9
Actualización automática o manual del antivirus	55%	11
Revisión de archivos descargados o enviados por el cliente	5%	1
Nada en particular	5%	1

Fuente: Elaboración propia, 2022.

Para lo relacionado con las aprobaciones necesarias para los procesos asociados a la política de gestión de antivirus, se consultó a los colaboradores sobre los roles o personas a los que acudirían en caso de necesitar información o requerir alguna aprobación relacionada con este tema; por tanto, en la Ilustración 15. Aprobación antivirus, se muestran los resultados obtenidos.

Ilustración 15. Aprobación antivirus



Fuente: Elaboración propia, 2022.

Se puede decir que la mayoría de los colaboradores expresaron que acudirían al líder de la tribu a la cual pertenecen. Se puede considerar eso como un único escalamiento, esto como primera instancia, seguido de la opción de consultarlo con el líder de su tribu y con Alex Ureña, lo que se traduce a dos escalamientos. En la Tabla 22. Resumen aprobación antivirus, se muestra un conglomerado de los resultados obtenidos.

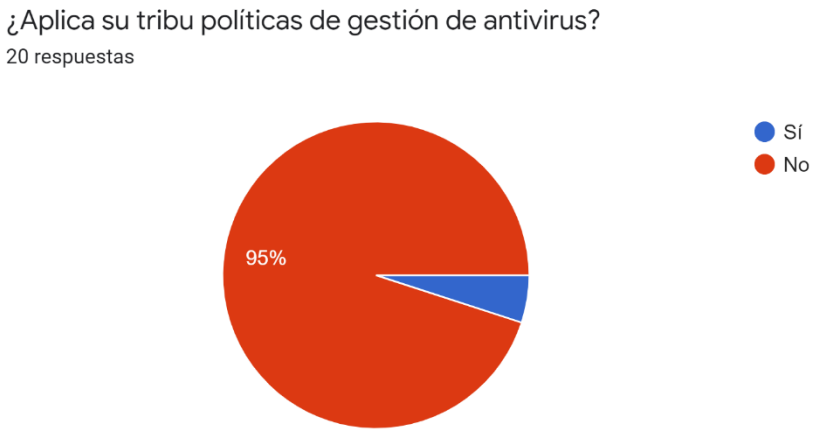
Tabla 22. Resumen aprobación antivirus

Respuesta	Escalamientos	Porcentaje	Total de colaboradores que respondieron
Con el líder de tribu	1	45%	9
Con el líder de tribu y Alex Ureña	2	30%	6
Sólo con Alex Ureña	1	15%	3
Con el líder de tribu, algún otro compañero y Alex Ureña	Al menos 3	10%	2

Fuente: Elaboración propia, 2022.

Para finalizar con esta política, es requerido conocer si alguna de las tribus existentes aplica procesos relacionados con la política de gestión de antivirus, a lo que un total del 95% de los colaboradores dieron un “No” como respuesta. En la Ilustración 16. Aplicación de procesos de antivirus, se muestra la distribución de porcentajes por respuesta dada.

Ilustración 16. Aplicación de procesos de antivirus



Fuente: Elaboración propia, 2022.

Por tanto, se puede concluir, según los resultados obtenidos, que un 95% de los colaboradores de las tribus no aplican procesos de gestión de antivirus, lo que en números se traduce a un total de 19 colaboradores de 20 entrevistados. En Tabla 23. Resumen aplicación de procesos antivirus, se puede evidenciar el total de respuestas recibidas.

Tabla 23. Resumen aplicación de procesos antivirus

Respuesta	Porcentaje	Total de colaboradores
No	5%	19
Sí	95%	1
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

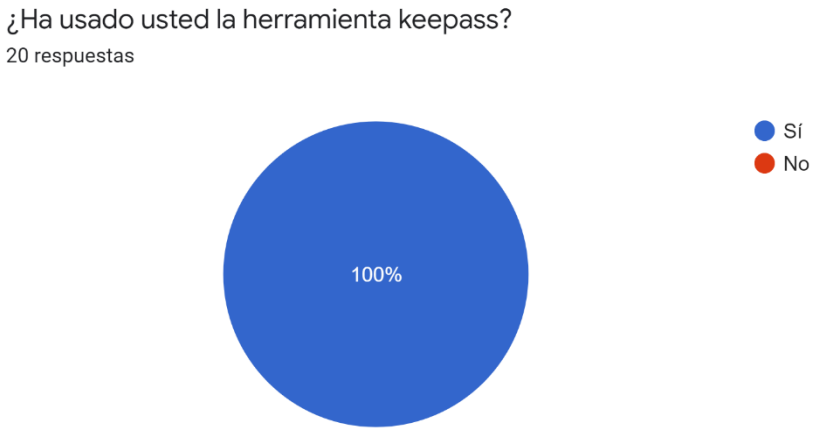
4.2.3 Control y uso de privilegios administrativos

En esta sección se detalla el análisis de la información obtenida de los instrumentos de investigación, en específico, para la política “Control y uso de privilegios administrativos”. Para esta política, actualmente en la organización se utiliza una herramienta llamada Keepass, sobre

la cual se detalla en la sección 2.7.1 Keepass. Por tanto, la aplicación de los instrumentos de investigación para recuperar la información sobre el estado actual de la empresa, respecto de esta política, se enfoca en el uso que actualmente se hace de esta herramienta en la organización.

Relacionado con el uso de la herramienta Keepass, el total de los veinte colaboradores encuestados aseguraron haber usado en alguna ocasión esta herramienta. En la Ilustración 17. Uso de keepass, se muestra la gráfica que valida los datos mencionados.

Ilustración 17. Uso de keepass



Fuente: Elaboración propia, 2022.

A modo resumen, en la Tabla 24. Resumen uso de keepass se muestran los datos desglosados sobre la Ilustración 17. Uso de keepass.

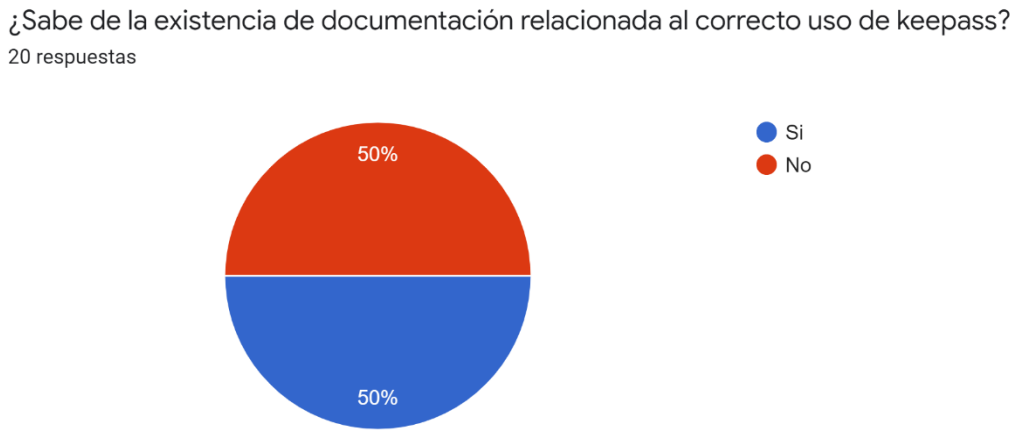
Tabla 24. Resumen uso de keepass

Respuesta	Porcentaje	Total de colaboradores
No	0%	0
Si	100%	20
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Para determinar si los colaboradores conocen sobre la existencia de documentación relacionada con Keepass en la organización, se realizó la consulta expuesta en la Ilustración 18. Documentación Keepass, en la cual se determina que el 50% de los encuestados no sabe si tal documentación existe.

Ilustración 18. Documentación Keepass



Fuente: Elaboración propia, 2022.

En términos de números de colaboradores, en la Tabla 25. Resumen documentación Keepass, se muestra que un total de diez colaboradores de 20 entrevistados, no sabe sobre la existencia de la documentación mencionada.

ati

Tabla 25. Resumen documentación Keepass

Respuesta	Porcentaje	Total de colaboradores
No	50%	10
Si	50%	10
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Con el fin de determinar los procesos que comúnmente realizan los colaboradores con la herramienta Keepass, en la Ilustración 19. Procesos keepass se enumeran algunos de estos.

Ilustración 19. Procesos keepass

Fuente: Elaboración propia, 2022.

Por tanto, en la Tabla 26. Resumen procesos keepass, se muestra el detalle de los procesos mencionados por los colaboradores, así como el número de personas que seleccionó cada uno de los procesos y su porcentaje, según el total de encuestas aplicadas.

ati

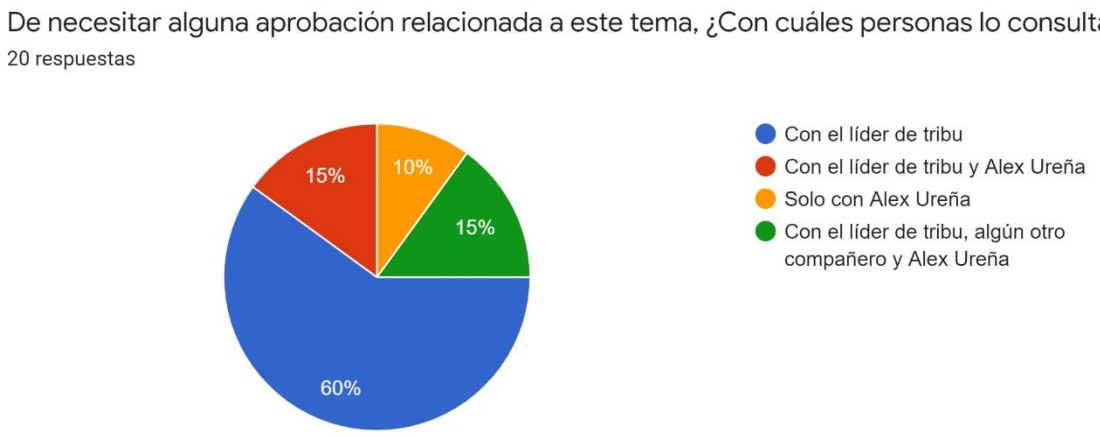
Tabla 26. Resumen procesos keepass

Respuesta	Porcentaje	Total de colaboradores
Consulta de usuarios	95%	19
Agregar usuarios	85%	17
Eliminar usuarios	25%	5
Sincronización de usuarios	90%	18
Consulta de URL's de ambientes	5%	1
Ver/editar/agregar URL's de acceso a ambientes	5%	1
Editar usuarios	5%	1

Fuente: Elaboración propia, 2022.

Para las aprobaciones necesarias en temas de la herramienta Keepass, los encuestados determinaron que en su mayoría lo consultarían con el líder de tribu, lo cual se traduce a un escalamiento. En la Ilustración 20. Aprobaciones keepass, se muestra el total de respuestas brindadas por los colaboradores.

Ilustración 20. Aprobaciones keepass



Fuente: Elaboración propia, 2022.

Para un mejor desglose de las respuestas obtenidas, en la Tabla 27. Resumen aprobaciones keepass, se muestra el total de respuestas brindadas junto con el número de colaboradores que las seleccionaron, además de su relación porcentual según el total de encuestados.

Tabla 27. Resumen aprobaciones keepass

Respuesta	Escalamientos	Porcentaje	Total de colaboradores que respondieron
Con el líder de tribu	1	60%	12
Con el líder de tribu y Alex Ureña	2	15%	3
Sólo con Alex Ureña	1	10%	2
Con el líder de tribu, algún otro compañero y Alex Ureña	Al menos 3	15%	3

Fuente: Elaboración propia, 2022.

4.2.4 Inventario y control de los activos de software.

En esta sección se brindan detalles sobre el análisis de la información obtenida de los instrumentos de investigación, en específico, para la política propuesta “Inventario y control de los activos de software”.

Concerniente a la existencia de documentación sobre inventarios de los activos de software de la organización, en la Ilustración 21. Documentación inventario de activos de software se muestran las respuestas brindadas por los colaboradores; destaca que un 70% dio un “No” como respuesta.

Ilustración 21. Documentación inventario de activos de software

Fuente: Elaboración propia, 2022.

En la Tabla 28. Resumen inventario de activos de software, se muestra el resumen de las respuestas brindadas con su respectivo número de colaboradores y su porcentaje sobre el total de entrevistados.

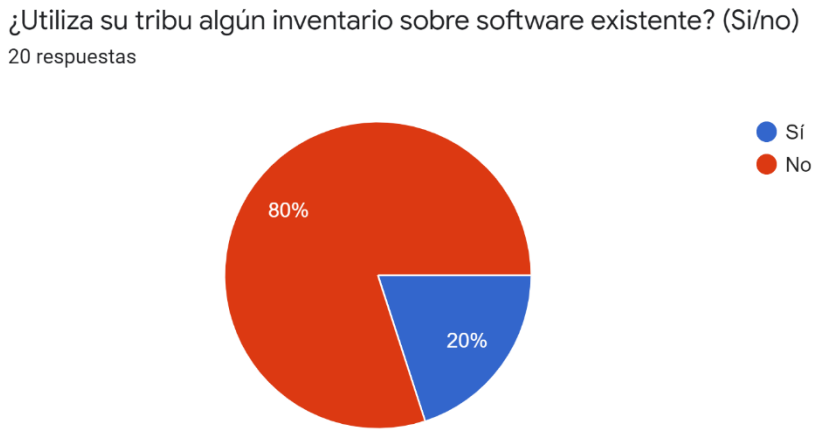
Tabla 28. Resumen inventario de activos de software

Respuesta	Porcentaje	Total de colaboradores
No	70%	14
Si	30%	6
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Posteriormente, se consultó a los colaboradores si la tribu a la cual pertenecen dispone de algún inventario o repositorio en el cual se desglosen los activos de software de la organización y según las respuestas obtenidas, un 80% respondió "No". En la Ilustración 22. Utilización de inventario de software en tribus se encuentra el total de respuestas obtenidas.

Ilustración 22. Utilización de inventario de software en tribus



Fuente: Elaboración propia, 2022.

En la Tabla 29. Resumen utilización inventario de software en tribus, se presentan ambas respuestas obtenidas, así como la cantidad de colaboradores que seleccionó cada una de estas.

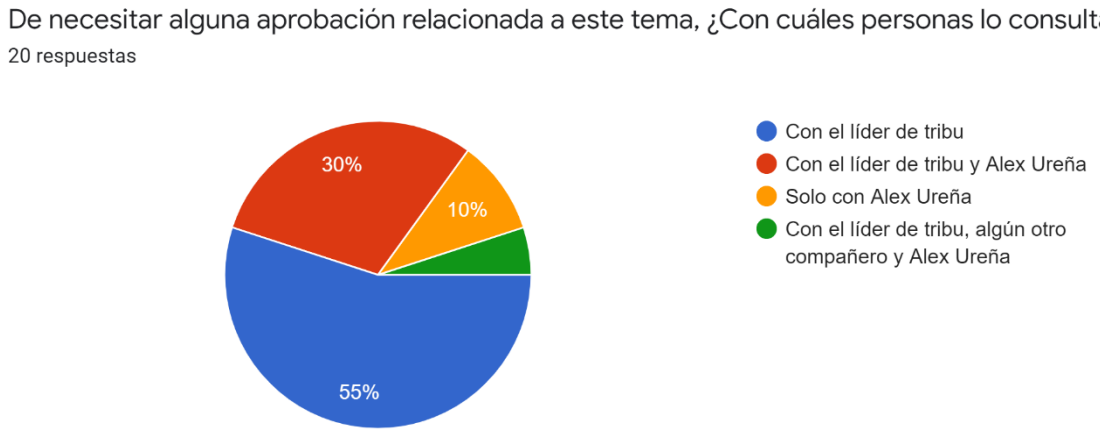
Tabla 29. Resumen utilización inventario de software en tribus

Respuesta	Porcentaje	Total de colaboradores
No	80%	16
Si	20%	4
Total	**100%**	**20**

Fuente: Elaboración propia, 2022.

Relacionado con el tema de consultas y aprobaciones sobre activos de software en la organización, se preguntó a los colaboradores con quién lo consultarían, a lo que se obtuvo como respuesta, con mayor porcentaje, consultarlo con el líder de tribu. Esto se entiende como un único escalamiento. En la Ilustración 23. Aprobaciones inventario de activos de software se muestra el gráfico asociado a las respuestas restantes.

Ilustración 23. Aprobaciones inventario de activos de software



Fuente: Elaboración propia, 2022.

En la Tabla 30. Resumen aprobaciones inventario de activos de software, se muestra el total de colaboradores que seleccionaron cada una de las respuestas planteadas, así como el porcentaje que esto representa sobre el total de encuestados.

Tabla 30. Resumen aprobaciones inventario de activos de software

Respuesta	Escalamientos	Porcentaje	Total de colaboradores que respondieron
Con el líder de tribu	1	55%	11
Con el líder de tribu y Alex Ureña	2	30%	6
Sólo con Alex Ureña	1	10%	2
Con el líder de tribu, algún otro compañero y Alex Ureña	Al menos 3	5%	1

Fuente: Elaboración propia, 2022.

4.3 Procesos identificados

En esta sección se muestra el conglomerado de procesos identificados para cada una de las políticas delimitadas en 4.1 Delimitación de políticas y según la aplicación de los instrumentos de investigación mencionados en 3.7 Instrumentos de Investigación y, por tanto, tomando como base los datos obtenidos de dichos instrumentos y detallados en Apéndice J – Conglomerado de datos recopilados de encuesta.

4.3.1 Defensa contra software malicioso

Según la aplicación de los instrumentos de investigación y el análisis de datos expuestos en secciones anteriores, se determina que la Tabla 31. Procesos identificados para política de defensa contra software malicioso, envuelve los procesos identificados para la política de defensa contra software malicioso, por las siguientes razones:

- Según el análisis expuesto en la sección 4.2.2 Defensa contra software malicioso, se determina que la organización actualmente no cuenta con procesos establecidos para la aplicación de esta política. En la Tabla 20. Resumen existencia de política de uso de antivirus, queda en evidencia la no existencia de políticas relacionadas con la defensa contra software malicioso, además, en la Tabla 23. Resumen aplicación de procesos antivirus, se demuestra que las tribus no aplican algún tipo de proceso relacionado con esta política.
- Según la revisión documental descrita en el Apéndice H – Minuta RV 02 – 1504, en la organización no existe documentación que valide la existencia de procesos relacionados con la defensa contra software malicioso.
- Según lo expuesto en Tabla 21. Resumen procesos asociados a gestión de antivirus, se tomarán los procesos expuestos como los procesos identificados para esta política. Estos también se validan según lo indicado por los entrevistados en Apéndice D – Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804.

Tabla 31. Procesos identificados para política de defensa contra software malicioso

Número de proceso	Nombre de proceso
1	Análisis periódicos de los equipos.
2	Análisis de dispositivos externas.
3	Actualización automática o manual del antivirus.
4	Revisión de archivos descargados o enviados por el cliente.

Fuente: Elaboración propia, 2022.

4.3.2 Control y uso de privilegios administrativos

Según la aplicación de los instrumentos de investigación y el análisis de datos expuestos en secciones anteriores, se determina que en la Tabla 26. Resumen procesos keepass, se encuentran los procesos identificados por los usuarios para la política de control y uso de privilegios administrativos. En la Tabla 32. Procesos identificados por los usuarios para gestión de Keepass, se detallan los procesos identificados por los usuarios encuestados.

Tabla 32. Procesos identificados por los usuarios para gestión de Keepass

Número de proceso	Nombre de proceso
1	Consulta de usuarios
2	Agregar usuarios
3	Eliminar usuarios
4	Consulta de URL's de ambientes
5	Ver/agregar/editarURL's de acceso a ambientes
6	Modificación de usuarios

Fuente: Elaboración propia, 2022.

Por otra parte, en la Tabla 25. Resumen documentación Keepass, se expone que existe documentación en la organización la cual valida la existencia de procesos establecidos relacionados con la gestión de Keepass, por tanto, después de la revisión documental detallada en Apéndice G – Minuta RV 01 – 1504 se concluye que la organización cuenta con los procesos enumerados en la Tabla 33. Procesos existentes para gestión de Keepass.

Tabla 33. Procesos existentes para gestión de Keepass

Número de proceso	Nombre de proceso
1	Configuración inicial
2	Consulta de usuarios
3	Eliminar usuarios
4	Actualizar usuarios.
5	Crear usuario.

Fuente: Elaboración propia, 2022.

Por tanto, analizando la Tabla 32. Procesos identificados por los usuarios para gestión de Keepass contra la Tabla 33. Procesos existentes para gestión de Keepass, se concluye que los procesos enumerados en la Tabla 32. Procesos identificados por los usuarios para gestión de Keepass, ya se encuentran abarcados en los procesos existentes en la organización. Por tanto, en conclusión, los procesos incluidos en la Tabla 33. Procesos existentes para gestión de Keepass serán tomados como los procesos identificados para esta política.

4.3.3 Inventario y control de los activos de software

Para esta política, se determina que no existen procesos establecidos en la organización relacionados con el inventariado y control de los activos de software de la organización por las siguientes razones:

- Según la revisión documental descrita en el Apéndice I – Minuta RV 03 – 1604, se demuestra que en la base de conocimiento de la organización no hay documentación que valide la existencia de procesos sobre el manejo de inventarios y el control de los activos de software.

- De acuerdo con los datos obtenidos de la aplicación de los instrumentos de investigación los cuales se detallan en el Apéndice J – Conglomerado de datos recopilados de encuesta, se demuestra en la Tabla 28. Resumen inventario de activos de software, que en su mayoría los colaboradores encuestados no conocen datos sobre documentación que valide la existencia de procesos relacionados con esta política.
- Conforme con la información obtenida de la aplicación de los instrumentos de investigación, y la cual se puntualiza en Apéndice J – Conglomerado de datos recopilados de encuesta, se prueba en la Tabla 29. Resumen utilización inventario de software en tribus que, según la mayoría de los usuarios encuestados, en sus tribus no se aplican procesos relacionados con esta política.

En conclusión, para esta política los procesos se definen en 5 Propuesta de Solución, los cuáles serán determinados de acuerdo con lo que indiquen las buenas prácticas de la industria.

4.4 Diagramación As-Is

En esta sección se muestran los diagramas *As-Is* de los procesos identificados en 4.3 Procesos identificados y según lo expuesto en las revisiones documentales detalladas en el Apéndice G – Minuta RV 01 – 1504, el Apéndice H – Minuta RV 02 – 1504 y el Apéndice I – Minuta RV 03 – 1604. Los diagramas mostrados se encuentran desarrollados mediante la notación *BPMN,* la cual se describe en 2.6 BPMN.

4.4.1 Defensa contra software malicioso

Para la diagramación de los procesos *As-Is,* se determinó que esta política no cuenta con procesos establecidos en la organización que permitan su diagramación, esto por las siguientes razones:

- En cuanto a la existencia de procesos, en la Tabla 20. Resumen existencia de política de uso de antivirus, se muestra el conglomerado de los datos obtenidos según el instrumento de investigación aplicado, en el cual es evidente la no existencia de procesos asociados a esta política. Esto también se valida según lo indicado por los entrevistados en Apéndice D –

Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804 y en la revisión documental descrita en el Apéndice H – Minuta RV 02 – 1504.

- Relacionado con la aplicación de procesos, en la Tabla 23. Resumen aplicación de procesos antivirus se muestran los datos obtenidos de la aplicación de los instrumentos de investigación, donde se evidencia que el 95% de los usuarios indica que la tribu a la cual pertenecen no aplica procesos relacionados con la política indicada. Esto, además, se valida según lo indicado por los entrevistados en Apéndice D – Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804.

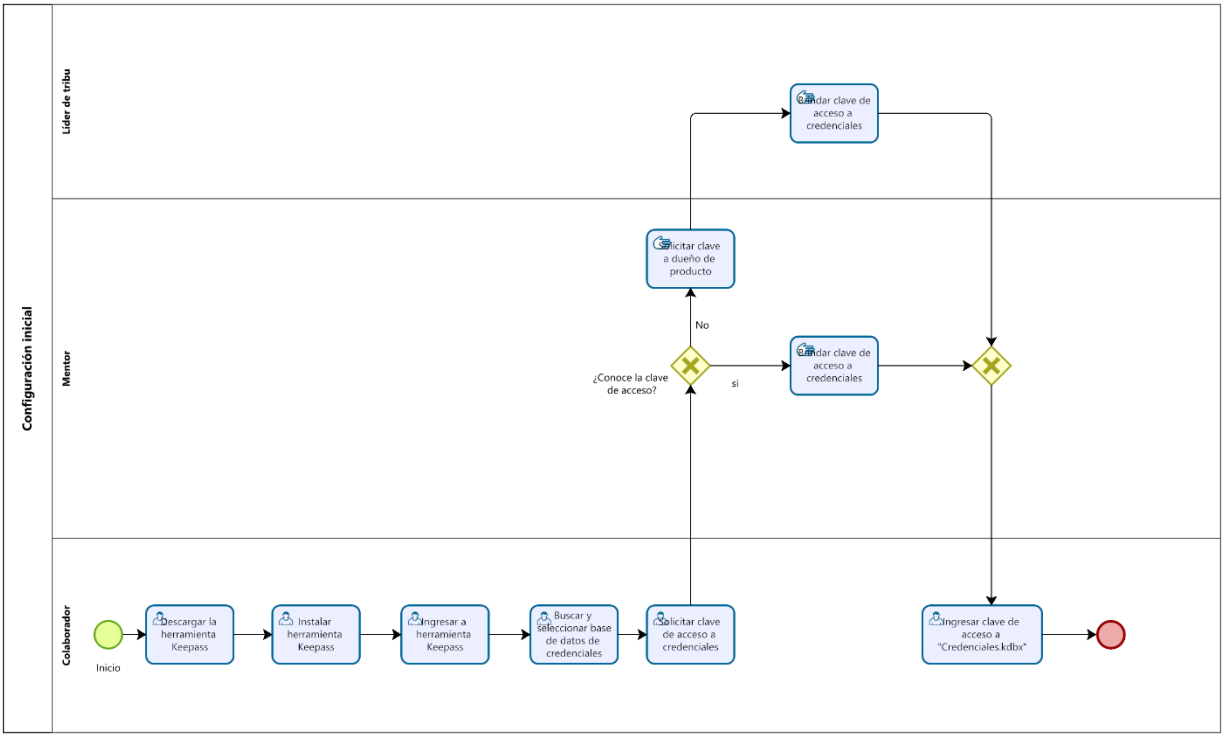
4.4.2 Control y uso de privilegios administrativos

En esta sección se muestran los diagramas *As-Is* de los procesos de la política de control y uso de privilegios administrativos. Los diagramas de los procesos mostrados corresponden a los listados en la Tabla 33. Procesos existentes para gestión de Keepass. Los diagramas expuestos en esta sección son realizados tomando como base la información obtenida de la revisión documental detallada en el Apéndice G – Minuta RV 01 – 1504.

4.4.2.1 Configuración inicial

Este proceso abarca las configuraciones iniciales por realizar para que los nuevos colaboradores cuenten con la herramienta Keepass en su equipo. En la Ilustración 24. Diagrama As-Is configuración inicial se muestra el diagrama del proceso mencionado.

Ilustración 24. Diagrama As-Is configuración inicial



Fuente: Elaboración propia, 2022.

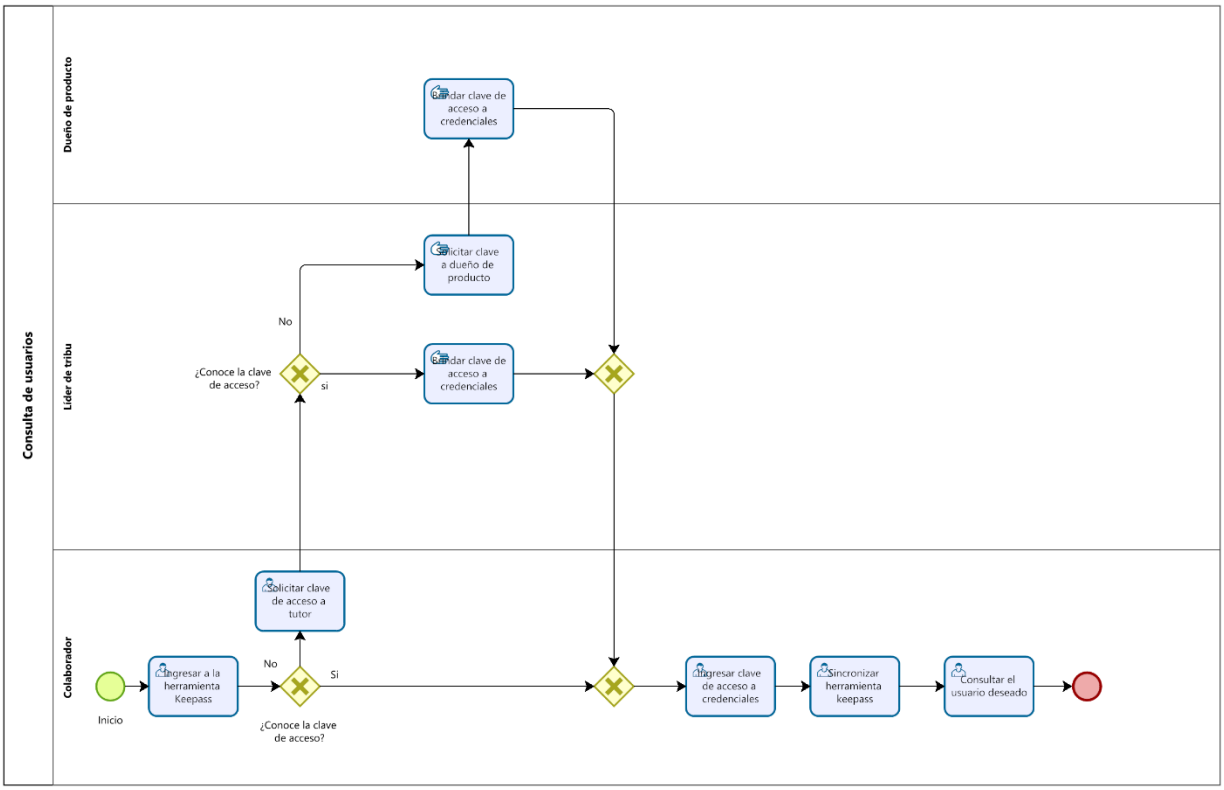
Entre las actividades más relevantes de este proceso se encuentran:

- Descargar la herramienta Keepass: El colaborador debe descargar la herramienta desde el enlace que se le fue enviado en el paquete de bienvenida a la organización.
- Buscar y seleccionar base de datos de credenciales: En el paquete de bienvenida se indica al colaborador la ruta del repositorio de documentos, en la cual se encuentra la base de datos que utiliza la herramienta Keepass. Esta tarea es muy importante ya que si no enlaza la base de datos no se podrá utilizar la herramienta.
- Solicitar clave de acceso a credenciales: La clave que desbloquea la base de datos de credenciales no se encuentra escrita en algún documento de la organización; esta clave está en propiedad de los miembros de la organización, por lo cual, el paso habitual es solicitarla a alguno de los usuarios determinados para esta actividad.

4.4.2.2 Consulta de usuarios

Este proceso consiste en secuenciar las actividades necesarias para consultar un usuario con el que se desea acceder a un ambiente en específico. En la Ilustración 25. Diagrama As-Is consulta de usuarios, se muestra el diagrama del desglose en actividades necesarias para llevar a cabo este proceso.

Ilustración 25. Diagrama As-Is consulta de usuarios



Fuente: Elaboración propia, 2022.

Entre las actividades relevantes de este proceso se encuentran:

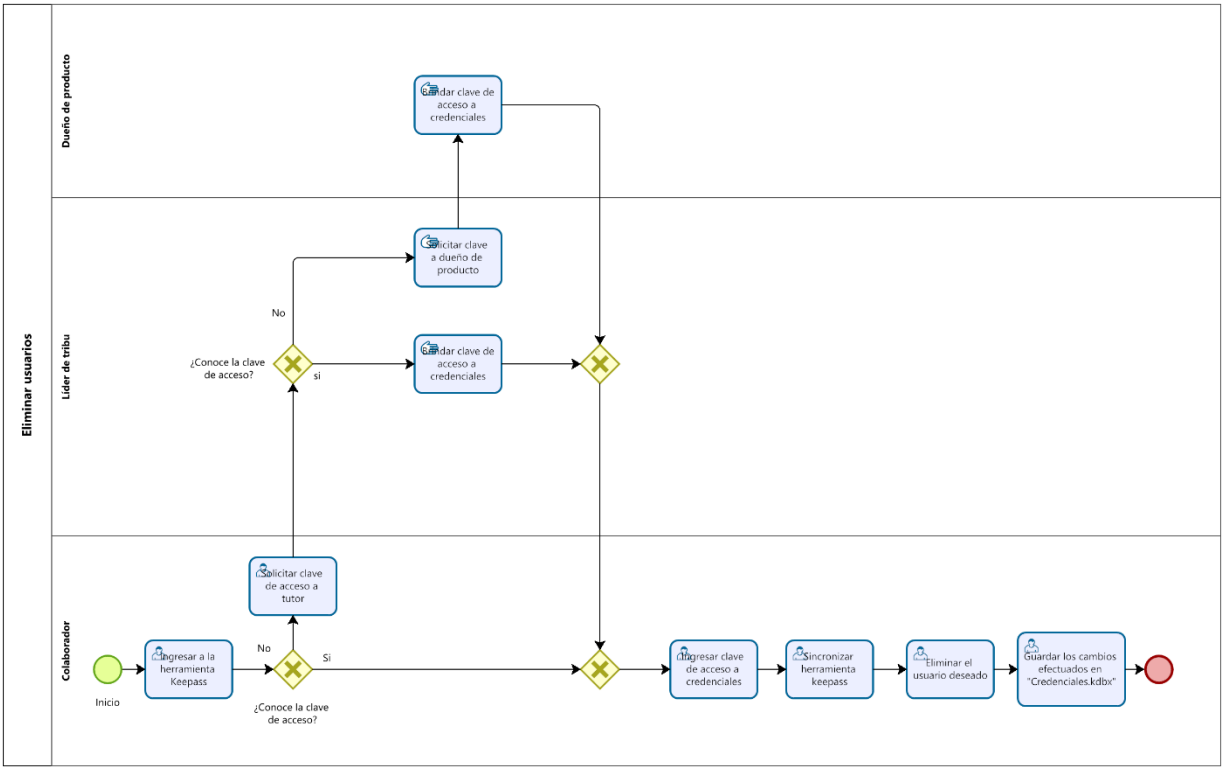
- Sincronizar herramienta Keepass: Esta actividad permite guardar y observar los cambios realizados sobre la base de datos de credenciales. Es de vital importancia, pues todos los usuarios que accedan a la herramienta tendrán la última versión de la base de datos.

- Consultar el usuario deseado: En la herramienta Keepass se almacenan usuarios de distintos tipos de herramientas, así como las cuentas de acceso de los colaboradores a los distintos ambientes de la cartera de clientes.

4.4.2.3 Eliminar usuarios

De acuerdo con la gestión normal de los clientes y de los usuarios, este proceso envuelve las actividades necesarias para efectuar la eliminación de un usuario en la herramienta Keepass. En la Ilustración 26. Diagrama As-Is eliminar usuario se muestran el total de actividades mencionadas.

Ilustración 26. Diagrama As-Is eliminar usuario



Fuente: Elaboración propia, 2022.

Como punto de atención, algunas de las actividades más importantes de este proceso son:

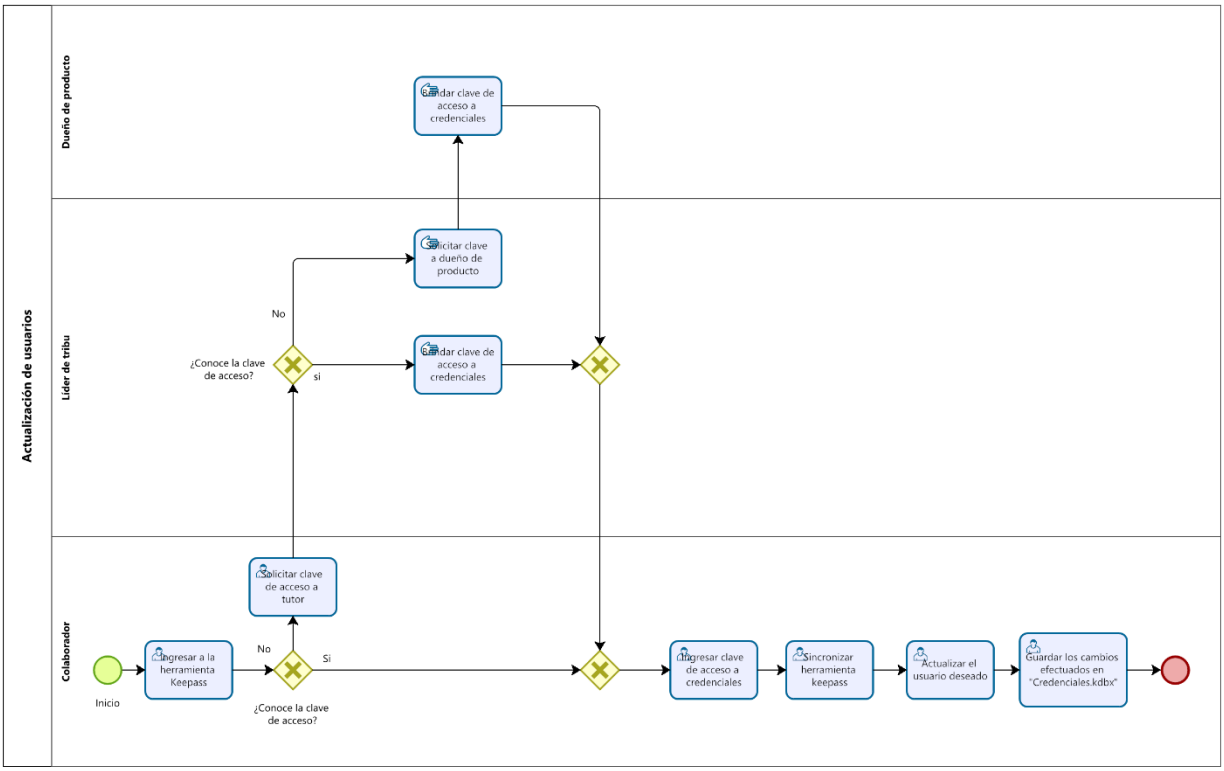
- Guardar los cambios efectuados en “Credenciales.kdbx”: El archivo “Credenciales.kdbx” es el equivalente a la base de datos en la cual se almacenan los usuarios creados, por tanto, al realizar algún cambio es de vital importancia guardarlo para que cuando los usuarios sincronicen la herramienta puedan ver la última actualización.

ati

4.4.2.4 Actualización de usuarios

El proceso en mención es utilizado para gestionar de buena manera los usuarios creados y que estos puedan estar actualizados para todos los usuarios que accedan a la herramienta. Este permite actualizaciones como el nombre de usuario, actualización de contraseña, dejar sobre el usuario alguna reseña importante o cambiar el ambiente al cual este se encuentra asociado. En la Ilustración 27. Diagrama As-Is actualización de usuarios se muestra el paso a paso para ejecutar este proceso satisfactoriamente.

Ilustración 27. Diagrama As-Is actualización de usuarios



Fuente: Elaboración propia, 2022.

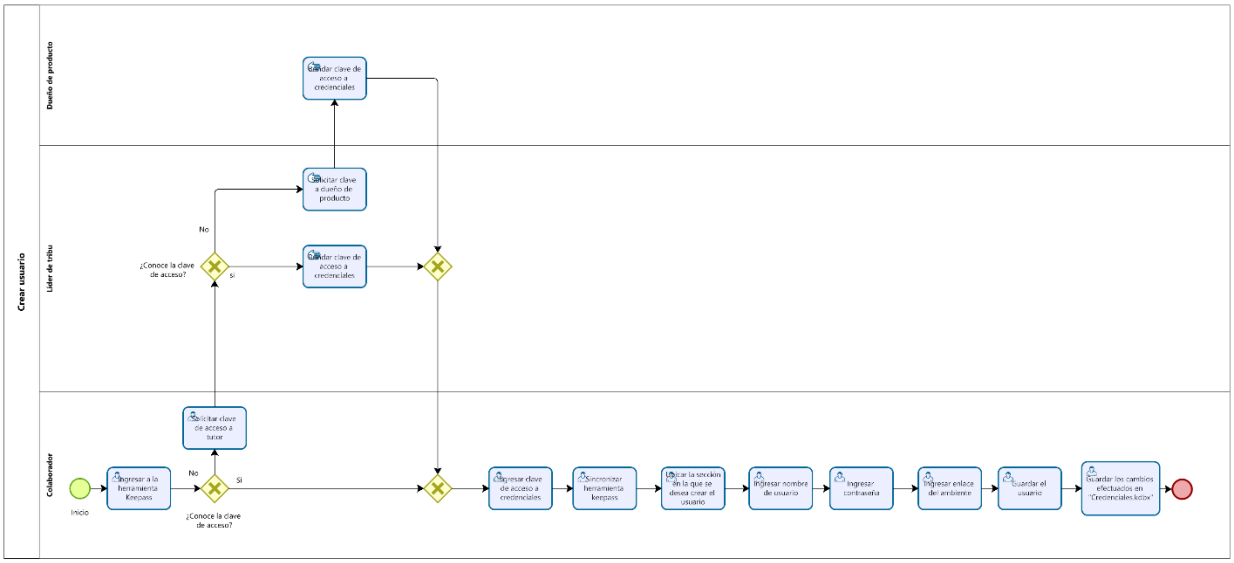
4.4.2.5 Creación de usuario

Este proceso es el conglomerado de actividades necesarias para crear un usuario en la herramienta Keepass. Durante el ciclo de vida de un proyecto es normal que el número de colaboradores participates de la implementación vaya creciendo conforme se avanza en el cronograma; por eso, a la herramienta Keepass se suelen agregar usuarios de forma cotidiana.

ati

En la Ilustración 28. Diagrama As-Is creación de usuario, se muestra el detalle de las actividades mencionadas.

Ilustración 28. Diagrama As-Is creación de usuario



Fuente: Elaboración propia, 2022.

4.4.3 Inventario y control de los activos de software.

Conforme con la presentación de los diagramas de los procesos *As-Is,* se determinó que esta política no cuenta con procesos establecidos en la organización que permitan detallar un diagrama, esto por las siguientes razones:

- En la sección Procesos identificados, específicamente en la sección 4.3.3 Inventario y control de los activos de software, se determinó que esta política no tiene procesos definidos, debido a la no existencia de procesos establecidos en la organización; esto también se comprueba según el Apéndice I – Minuta RV 03 – 1604 y en el análisis de los datos expuesto en Tabla 28. Resumen inventario de activos de software, en el cual se indica que los colaboradores no conocen sobre la existencia de documentación relacionada con los procesos ligados a esta política.

- En cuanto a la aplicación de los procesos, en la Tabla 29. Resumen utilización inventario de software en tribus, se muestra que según la mayoría de los colaboradores entrevistados, este tipo de procesos no se aplica en sus respectivas tribus.

4.5 Identificación de oportunidades de mejora

En este apartado se muestran los análisis requeridos para demostrar el puntaje de cada una de las políticas de seguridad propuestas; esto con la finalidad de determinar si presentan o no una oportunidad de mejora según los rubros especificados en la sección 3.2.3 Axiología.

4.5.1 Defensa contra software malicioso

Para demostrar la oportunidad de mejora relacionada con esta política, se toman en cuenta las siguientes premisas según los rubros definidos en 3.2.3 Axiología.:

- Para el rubro de documentación existente, en la Tabla 20. Resumen existencia de política de uso de antivirus, se evidencia que un 95% de los colaboradores entrevistados no conocen sobre la aplicación de procesos asociados a esta política. Además, según Tabla 23. Resumen aplicación de procesos antivirus, un 95% de los encuestados indican que su tribu no aplica dicha política. Por tanto, se puede determinar que la organización no cuenta con documentación sobre los procesos asociados a la política de defensa contra software malicioso. Además, en las entrevistas detalladas en las minutas Apéndice D – Minuta EM 03 – 0804 y Apéndice E – Minuta EM 04 – 1804 también se confirma lo ya mencionado. En conclusión, para esta política el rubro de documentación existente tiene un puntaje de 50%.
- Para el rubro de aprobaciones necesarias, en la Tabla 22. Resumen aprobación antivirus se muestra que, mayoritariamente, un 60% de los colaboradores entrevistados únicamente harían un escalamiento; se puede decir, por tanto, que para este rubro el puntaje sería de 5%.
- En cuanto al rubro de aplicación de la política en las distintas tribus de la organización, en la Tabla 23. Resumen aplicación de procesos antivirus, se muestra que un total del 95% de los entrevistados confirma la no aplicación de eta política en la organización, por tanto, se determina que al menos seis de las siete tribus existentes no aplican procesos

relacionados con la política de defensa contra software malicioso. Para este rubro se concluye que el puntaje de la política sería 35%.

En conclusión, y según se muestra en Tabla 34. Puntaje oportunidad de mejora Defensa contra software malicioso, el puntaje total de la política es de 90% y según lo definido en 3.2.3 Axiología, un puntaje mayor a 70% demuestra que la política tiene oportunidad de mejora, por tanto, se determina que la política de defensa contra software malicioso tiene oportunidad de mejora.

Tabla 34. Puntaje oportunidad de mejora Defensa contra software malicioso

Rubro	Puntaje obtenido
Documentación existente	50%
Aprobaciones necesarias	5%
Aplicación en tribus	35%
Total	90%

Fuente: Elaboración propia, 2022.

4.5.2 Control y uso de privilegios administrativos

Para el cálculo de la oportunidad de mejora relacionada con esta política, se toman en cuenta las siguientes premisas según los rubros definidos en 3.2.3 Axiología.:

- Para el rubro relacionado a la documentación existente, en la Tabla 25. Resumen documentación Keepass, se evidencia que un 50% de los colaboradores entrevistados conocen sobre documentación existente relacionada con procesos de esta política. Además, según la revisión documental desarrollada en el Apéndice G – Minuta RV 01 – 1504 se demuestra que sí existe documentación enfocada a esta política, por tanto, para esta política el rubro de documentación existente tiene un puntaje de 10%.

- Para el rubro de aprobaciones necesarias, la Tabla 27. Resumen aprobaciones keepass, muestra que, mayoritariamente, un 45% de los colaboradores entrevistados únicamente harían un escalamiento, por lo que se puede decir que para este rubro el puntaje sería de 5%.
- En cuanto al rubro de aplicación de la política en las distintas tribus de la organización, en la Tabla 24. Resumen uso de keepass, se evidencia que el total de los entrevistados confirma haber utilizado la herramienta keepass; por tanto, se determina que las siete tribus existentes aplican procesos relacionados al uso de Keepass. Para este rubro se concluye que el puntaje de la política sería 5%. Además, este rubro se valida también con los criterios registrados en las entrevistas aplicadas, las cuales llevan como prueba el Apéndice D – Minuta EM 03 – 0804 y el Apéndice E – Minuta EM 04 – 1804.

En conclusión, y según se muestra en la Tabla 35. Puntaje oportunidad de mejora Control y uso de privilegios administrativos, el puntaje total de la política es de 20% y según lo definido en 3.2.3 Axiología, un puntaje mayor a 70% demuestra que la política tiene oportunidad de mejora; por tanto, se determina que la política de control y uso de privilegios administrativos tiene una baja oportunidad de mejora.

Tabla 35. Puntaje oportunidad de mejora Control y uso de privilegios administrativos

Rubro	Puntaje obtenido
Documentación existente	10%
Aprobaciones necesarias	5%
Aplicación en tribus	5%
Total	20%

Fuente: Elaboración propia, 2022.

4.5.3 Inventario y control de los activos de software.

Para el análisis de la oportunidad de mejora relacionada con esta política, se toman en cuenta las siguientes premisas según los rubros definidos en 3.2.3 Axiología.:

- En cuanto al rubro de documentación existente, en la Tabla 28. Resumen inventario de activos de software, se evidencia que un 70% de los colaboradores entrevistados no conocen sobre documentación existente relacionada con procesos de esta política. Además, según la revisión documental desarrollada en el Apéndice I – Minuta RV 03 – 1604, se demuestra que no existe documentación enfocada a esta política, por tanto, se determina que el rubro de documentación existente tiene un puntaje de 50%.
- Para el rubro de aprobaciones necesarias, en la Tabla 30. Resumen aprobaciones inventario de activos de software, se muestra que un 55% de los colaboradores entrevistados únicamente harían un escalamiento; se puede decir que para este rubro el puntaje sería de 5%.
- En cuanto al rubro de aplicación de la política en las tribus de la organización, en la Tabla 29. Resumen utilización inventario de software en tribus, un del total del 80% de los entrevistados confirma que no se utiliza esta política en la tribu a la cual pertenece, por tanto, se determina que ninguna de las tribus existentes aplica procesos relacionados con inventarios de los activos de software. Para este rubro se concluye que el puntaje de la política sería 35%. Este rubro se valida con los criterios registrados en las entrevistas aplicadas que llevan como prueba el Apéndice D – Minuta EM 03 – 0804 y el Apéndice E – Minuta EM 04 – 1804.

Para concluir, y según se muestra en la Tabla 36. Puntaje oportunidad de mejora Inventario y control de Activos de software, el puntaje total de la política corresponde a 90% y según lo definido en 3.2.3 Axiología, un puntaje mayor a 70% demuestra que la política tiene oportunidad de mejora, por tanto, se determina que la política de inventario y control de los activos de software tiene oportunidad de mejora.

Tabla 36. Puntaje oportunidad de mejora Inventario y control de Activos de software

Rubro	Puntaje obtenido
Documentación existente	50%
Aprobaciones necesarias	5%
Aplicación en tribus	35%
Total	90%

Fuente: Elaboración propia, 2022.

4.6 Construcción de la propuesta de solución

Según los distintos puntos definidos en el capítulo Análisis de Resultados, es necesario determinar las estrategias a tomar en cuenta para la construcción de la propuesta a detallar en el capítulo 5 Propuesta de Solución, esto basado en las fases y actividades definidas en la sección 3.8 Procedimiento metodológico de la Investigación, así como los instrumentos de investigación definidos para cada fase en la Tabla 16. Operalización de las variables. Siendo así, la propuesta de construcción se define bajo los siguientes puntos:

- Según lo determinado en 4.3 Procesos identificados, es necesario tomar dichos procesos y analizarlos según el marco de referencia 2.2 COBIT 5 para determinar la brecha existente entre la situación actual y lo mencionado por el marco de referencia.
- Una vez determinada la brecha, se debe hacer el modelado de los procesos *To-be* basados en la brecha identificada, esto mediante la utilización de la metodología descrita en el apartado 2.5 Gestión de procesos de negocio (BPM) y bajo la notación 2.6 BPMN.
- Una vez diagramados los procesos *To-be,* se debe llevar a cabo la simulación de los procesos pertenecientes a cada una de las políticas, esto enfocado en los recursos utilizados y mediante la herramienta 2.7.3 Bizagi Modeler. Según la política, se presentan los siguientes escenarios:
    - Para la política de “Defensa contra software malicioso” y la política de “Inventario y control de los activos de software” no se incluirá simulación, dado que corresponden a procesos y políticas nuevas, que no tienen arraigo en la organización y que los colaboradores no podrán apoyar en las labores de determinar tiempos asociados. Esto se complementa con los hallazgos de la revisión documental descrita en Apéndice Q - Minuta RV 04 – 2208, y en la decisión tomada en conjunto con la organización descrita en el Apéndice O - Minuta EM 08 – 2308.

- Para la política de “Control y uso de privilegios administrativos” se realizará la respectiva simulación del escenario *As-Is* y el escenario *To-be*.

- Posterior Al modelado de los procesos, se abarcará la medición de la efectividad sobre los procesos *To-be* de las políticas. Esta medición se realizará basado en los rubros definidos en la sección 3.2.3 Axiología.
- Relacionado al análisis financiero, se realiza lo siguiente dependiendo de la política:
  - Para la política de “Control y Uso de privilegios administrativos” se realiza el análisis financiero basado en los resultados obtenidos de las simulaciones de los escenarios *As-Is* y *To-be.*
  - Para la política de “Defensa contra software malicioso”, el análisis financiero se realiza tomando como base la investigación detallada en el Apéndice R – Minuta RV 05 – 2308, en la cual se muestran los hallazgos necesarios para la realización del análisis financiero de esta política, basado en las ganancias y pérdidas de la no protección de los equipos.
  - Relacionado a la política de “Inventario y control de los activos de software”, el análisis financiero estará basado en la investigación detallada en el Apéndice S – Minuta RV 06 – 2408, en el cual, según se muestra en los hallazgos, se asocian ganancias y pérdidas relacionadas al no control de los activos de software.

5 Propuesta de Solución

Este capítulo tiene como principal objetivo describir las soluciones propuestas para los hallazgos descritos en Análisis de Resultados. Así mismo, en esta sección se desarrollan las actividades necesarias para la culminación de la segunda y tercera fases de este proyecto, descritas las secciones Fase 2. Identificación de la brecha y Fase 3. Medición de efectividad.

5.1 Definición de la brecha relacionada con procesos existentes

En esta sección se describen los procesos que se proponen como parte de cada una de las políticas de seguridad descritas. Para la selección de estos procesos se toman como base los definidos en 4.3 Procesos identificados, los cuales forman parte de la situación actual de la empresa, contra lo que dicta el marco de referencia descrito en la sección 2.2 COBIT 5.

5.1.1 Defensa contra software malicioso

En la sección 4.3.1 Defensa contra software malicioso, se hace referencia a los procesos identificados para esta política, según los resultados obtenidos de la aplicación de los instrumentos de investigación, los cuales se detallan en el Apéndice J – Conglomerado de datos recopilados de encuesta. Tomando los procesos descritos en la Tabla 31. Procesos identificados para política de defensa contra software malicioso, y comparándolos con lo descrito por el marco de referencia COBIT 5, específicamente en DSS05.01 Proteger contra software malicioso (malware), ISACA (2012) se determina una serie de actividades, enumeradas en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware), las cuales permiten llegar a los siguientes resultados:

- Se agrega el proceso denominado “Configuración inicial de antivirus”, esto para cubrir la primera actividad, la cual se puede visualizar en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware) y en la que ISACA (2012). Se recomienda implementar procedimientos que prevengan ataques de software malicioso, además de generar concienciación sobre los colaboradores de la organización acerca de la importancia de proteger sus equipos. Por tanto, este proceso pretende que, una vez ingresado el nuevo colaborador, se empiecen a abordar procesos de protección contra

software malicioso, aumentando la prevención y generando concienciación sobre el tema desde que se ingresa a la organización. Además, este mismo proceso cubre la segunda actividad visualizada en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware), en la cual el marco de referencia COBIT 5 indica, a través de ISACA (2012), que se deben instalar en los equipos de la organización herramientas que permitan proteger los activos contra software malicioso. Siendo así, el proceso de "Configuración inicial de antivirus" funciona como guía que facilita la instalación de herramientas contra software malicioso en los equipos por considerar.

- Se agrega a la política el proceso llamado "Análisis de validez del antivirus ante nuevas amenazas", esto para abarcar la cuarta actividad visible en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware). En esta actividad ISACA (2012) recomienda estar alerta sobre nuevas amenazas que puedan surgir y que pongan en riesgo a la organización. Con este nuevo proceso, el cual debe ser ejecutado periódicamente, el colaborador encargado deberá validar la situación actual del programa antivirus ante las nuevas amenazas existentes.

- Para la sexta actividad, visible en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware), ISACA (2012) menciona la importancia de formar, de manera periódica, a los colaboradores, para que estén al tanto sobre los riesgos del software malicioso presente en Internet y en los correos electrónicos. Para abarcar esta actividad, se reenfocará el proceso denominado "Revisión de archivos descargados o enviados por el cliente", el cual se puede visualizar en la Tabla 31. Procesos identificados para política de defensa contra software malicioso, para que incluya la actividad denominada "Descargar el archivo de su ruta o email origen", la cual involucra la prevención contra amenazas provenientes del correo electrónico utilizado por la organización.

Según lo expresado en la Apéndice L - Minuta EM 06 – 1706, la organización descarta la tercera y la quinta actividades para la propuesta en este proyecto, por las siguientes razones:

- Para la tercera actividad, la cual puede ser visualizada en la Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware), se determina que no forma parte de la propuesta debido a que la organización no cuenta con la infraestructura tecnológica necesaria para su aplicación.
- En cuanto a la quinta actividad, visible en Ilustración 7. Actividades de DSS05.01 Proteger contra Software malicioso (malware), se comenta que se descarte de esta propuesta debido a que la organización no cuenta con el nivel de madurez suficiente para su implementación.

En la Tabla 37. Procesos propuestos para política de defensa contra software malicioso, se desglosan los procesos propuestos en su versión final, según los cambios propuestos en la identificación de la brecha.

Tabla 37. Procesos propuestos para política de defensa contra software malicioso

Número de proceso	Nombre de proceso
1	Configuración inicial de antivirus
2	Análisis periódicos de los equipos.
3	Análisis de dispositivos externos.
4	Actualización automática o manual del antivirus.
5	Revisión de archivos descargados o enviados por el cliente.
6	Análisis de validez del antivirus ante nuevas amenazas

Fuente: Elaboración propia, 2022.

5.1.2 Control y uso de privilegios administrativos

Según la situación actual de la organización, en la sección 4.3.2 Control y uso de privilegios administrativos se enumeran los procesos identificados para esta política, los cuales se determinan según los resultados obtenidos de la aplicación de los instrumentos de investigación y cuyos resultados pueden ser consultados en la sección Apéndice J – Conglomerado de datos recopilados de encuesta, si se toman como referencia los procesos descritos en la Tabla 32. Procesos identificados por los usuarios para gestión de Keepass y se compara contra el marco de referencia COBIT 5, detallado en DSS05.04 Gestionar la identidad del usuario y el acceso lógico. ISACA (2012) enumera las actividades necesarias para su cumplimiento, las cuales se exponen en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico; estas, según su análisis, permiten llegar a las siguientes conclusiones:

- Para la primera actividad, visualizable en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, ISACA (2012) señala que se debe tener referenciado, al asignar accesos, lo que en el marco de referencia se señala como "necesidad de tener" y "necesidad de conocer". Esto, con la finalidad de tener conocimiento sobre si el acceso por brindar es realmente necesario para el usuario que lo solicita. Para cumplir con esta actividad, se agregará al proceso "Crear usuario", el cual es señalado como un proceso, identificado en la Tabla 33. Procesos existentes para gestión de Keepass. La actividad "Analizar requerimiento de creación de usuario" tiene el principal objetivo que el "Líder de tribu" valide y cuestione la creación del usuario; la actividad "Brindar respuesta al colaborador" dará respuesta al colaborador sobre si es necesario crear o no el usuario.
- Para el cumplimiento de la cuarta actividad, la cual es parte del marco de referencia según se muestra en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, se menciona por parte de ISACA (2012), que los cambios relacionados con eliminar, crear, o modificar accesos, deben ser efectuados en el momento oportuno y bajo su debida aprobación. Para su cumplimiento, se tomarán los procesos "Crear

Usuario", "Actualizar usuarios" y "Eliminar usuarios" los cuales están definidos como procesos identificados en la situación actual de la organización, mostrada en la Ilustración 27. Diagrama As-Is actualización de usuarios y se agregarán a estos las actividades necesarias para velar por el cumplimiento de lo dictado por esta actividad. Por tanto, para el proceso "Crear usuario" se agrega la actividad "Analizar requerimiento de creación de usuario" en la cual el líder de tribu aprueba la creación del usuario. Para el proceso "Actualizar usuarios" se agrega la actividad "Analizar requerimiento de actualización de usuario" en la cual el líder de la tribu aprobará sobre la actualización por realizar y para el proceso de "Eliminar usuarios" se agrega la actividad "Analizar requerimiento de borrado del usuario", donde el líder de la tribu aprueba si es adecuado eliminar el usuario en cuestión.

- Para la sexta actividad, visible en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, ISACA (2012) expresa la necesidad de que un actor de la organización realice revisiones sobre los accesos brindados. Para el cumplimiento de esta actividad, se agregará a la política el proceso llamado "Revisión de usuarios", el cuál involucrará las actividades necesarias para la revisión efectiva de los usuarios y accesos brindados.
- Relacionado con la séptima actividad, de la cual se hace referencia en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, ISACA (2012) señala la importancia de que cada acceso sea unívoco, por tanto, es necesario que para el cumplimiento de esta actividad se agregue al proceso "Crear usuario", definido como proceso identificado en la Tabla 33. Procesos existentes para gestión de Keepass. Hay actividades necesarias para determinar si el usuario se encuentra creado actualmente. Siendo así, al proceso "Crear usuario" se agrega la actividad "Analizar requerimiento de creación de usuario" en la cual el líder de la tribu realizará la revisión de los accesos con el objetivo de asegurar que el usuario por crear no existe; como paso siguiente, informará al colaborador sobre la aprobación o denegación del requerimiento. Además, sobre el proceso "Revisión de usuarios" el cual es un proceso nuevo, se deben establecer parámetros de revisión relacionados con determinar si un usuario se encuentra repetido.

En relación con las actividades descartadas, en la Apéndice L - Minuta EM 06 – 1706, la organización brinda los motivos por los cuales no deben ser tomadas en la propuesta, las cuales se despliegan a continuación:

- Se descarta la segunda actividad, visible en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, dado que la estructura organizacional impide que, de momento, existan roles funcionales para gestión de la tarea tal y como lo solicita el marco de referencia.
- Para la tercera actividad, disponible en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, el colaborador comenta que es imposible establecer este tipo de controles, pues tamaño actual de la empresa impide que se establezcan unidades de negocio por separado. Sin embargo, considera que es un punto para tomar en cuenta a futuro según el crecimiento de la organización.
- Respecto a la quinta actividad, la cual se puede ver en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, se comenta que no es posible establecer la segregación solicitada en la actividad debido a que, por políticas internas, la información sobre la cual se realiza la propuesta de esta política es de libre acceso para todos los miembros de la organización.
- Para finalizar la octava actividad, visible en la Ilustración 6. Actividades de DSS05.04 Gestionar la identidad del usuario y el acceso lógico, se menciona el descarte de esta, debido a que la información sobre la cual se basa la política propuesta es de libre acceso y no se puede establecer sobre esta, procesos de auditoría.

En la Tabla 38. Procesos propuestos para política de control y uso de privilegios administrativos se enumeran los procesos propuestos como versión final para la política de control y uso de privilegios administrativos.

Tabla 38. Procesos propuestos para política de control y uso de privilegios administrativos

Número de proceso	Nombre de proceso
1	Configuración inicial
2	Consulta de usuarios
3	Eliminar usuarios.
4	Actualizar usuarios
5	Crear usuario.
6	Revisión de usuarios.

Fuente: Elaboración propia, 2022.

5.1.3 Inventario y control de los activos de software.

De acuerdo con el análisis de la situación actual, en la sección 4.3.3 Inventario y control de los activos de software, se desglosan las razones por las cuales la organización no cuenta con procesos establecidos o identificados mediante la aplicación de cada uno de los instrumentos de investigación. Por tanto, al comparar tal situación con lo expresado por el marco de referencia COBIT 5, lo cual se detalla en la sección BAI09.01 Identificar y registrar activos actuales, se concluye en lo siguiente:

- Para la primera actividad, visible en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales, se creará el proceso "Registro de activos de software", ya que según señala ISACA (2012), el objetivo de esta primera actividad es que la organización tenga la potestad de identificar todos los activos de software con los que cuente. Por tanto, este proceso contendrá todas las actividades necesarias para un registro efectivo de los activos de software.

- Tomando en cuenta la segunda actividad, la cual se puede visualizar en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales, ISACA (2012) se detalla como la gestión necesaria a efectuar de los requisitos legales, contractuales o reglamentarios asociados a los activos de software. Para cumplir con esta tarea, sobre el proceso llamado "Registro de activos de software", el cual se indicó en el punto anterior que será un proceso nuevo por crear, se deben incluir las actividades necesarias para asegurar la recopilación de la información legal o contractual del activo de software por registrar. Esta recopilación de aspectos legales y contractuales se hará con la actividad "Agregar información reglamentaria/contractual".
- Para la tercera actividad definida por ISACA (2012) como la necesidad de hacer revisiones de forma periódica para determinar la existencia de todos los activos de software y la cual es observable en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales, se propone la creación del proceso "Control de activos de software" en donde se establecerán actividades para la constante revisión del inventario de activos de software contra los existentes.
- Para el cumplimiento de la sexta actividad, la cual ISACA (2012) detalla la importancia de asegurar la contabilización de los activos. Se agregará al proceso "Registro de activos de software" la actividad "Asignar numeración al activo" la cual es necesaria para que al registrar un activo de software se le brinde a este su respectiva numeración.

  Por otra parte, es necesaria la creación del proceso "Revisión de numeración de activos de software" el cual es utilizado dentro del proceso "Control de activos de software" y que tiene como objetivo realizar el conteo de activos de software existentes. Esta sexta actividad del marco de referencia COBIT 5 puede ser visualizada en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales.

En cuanto a las actividades descartadas, en la Apéndice L - Minuta EM 06 – 1706 se establecen los motivos por los cuales no se tomaron en cuenta estas actividades para la propuesta de política. A continuación, se detallan las razones mencionadas:

- Se descarta la quinta actividad, visible en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales, debido a que, como se trata de un proceso nuevo, la organización no cuenta con el nivel de madurez suficiente para medir el aporte de valor de los activos y su vida útil restante.
- La cuarta actividad, la cual puede ser visualizada en la Ilustración 5. Actividades de BAI09.01 Identificar y registrar activos actuales, se descarta debido a que, al tratarse de un proceso nuevo, la organización no tiene establecidos objetivos sobre cada uno de los activos de software.

En la Tabla 39. Procesos propuestos para política de inventario y control de activos de software, se muestra el resumen de procesos propuestos para estas políticas.

Tabla 39. Procesos propuestos para política de inventario y control de activos de software

Número de proceso	Nombre de proceso
1	Registro de activos de software
2	Control de activos de software
3	Eliminar un activo de software
4	Revisión de numeración de activos de software

Fuente: Elaboración propia, 2022.

5.2 Modelado To-Be

En esta sección se detallan los modelos de procesos definidos para cada una de las políticas según la brecha identificada y detallada en las secciones 5.1.1 Defensa contra software malicioso, 5.1.2 Control y uso de privilegios administrativos y 5.1.3 Inventario y control de los activos de software. Para cada una de las políticas se plantean los determinados procesos acorde con las buenas prácticas del mercado. La realización de los diagramas *To-Be* busca la simplicidad de los procesos para el entendimiento general de todos los usuarios de la organización, así como la construcción de estos procesos acorde con las buenas prácticas de la industria adaptadas a la cultura de la organización.

5.2.1 Control y uso de privilegios administrativos

Para esta política se tomaron como procesos finales los determinados en la Tabla 38. Procesos propuestos para política de control y uso de privilegios administrativos. Estos procesos fueron determinados de acuerdo con la identificación de la brecha descrita en la sección 5.1.2 Control y uso de privilegios administrativos. El objetivo de esta sección es detallar, a nivel de actividad, cada uno de los procesos que son parte de esta política.

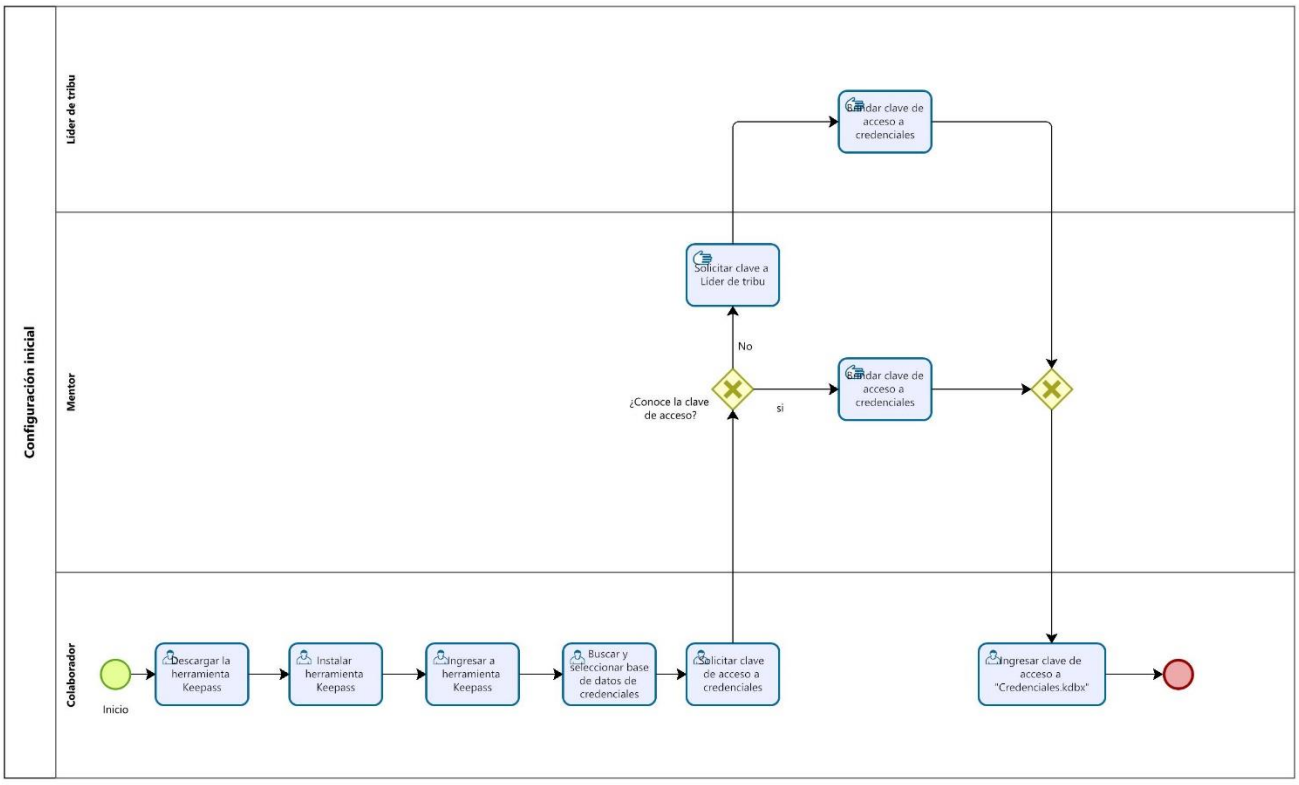
5.2.1.1 Configuración inicial

Este proceso tiene la finalidad de brindar guía sobre la configuración inicial que se debe llevar a cabo para utilizar la herramienta Keepass, descrita en la sección 2.7.1 Keepass, la cual es utilizada por la organización como el gestor de los accesos y contraseñas. En la Ilustración 29. Proceso Configuración Inicial se muestra el diagrama del proceso especificado, el cual contiene las siguientes actividades:

- Descargar la herramienta Keepass: Proceder con la descarga de la herramienta Keepass en el dispositivo brindado al colaborador.
- Instalar herramienta Keepass: Instalar la herramienta Keepass, previamente descargada, en el correspondiente equipo.
- Ingresar a herramienta Keepass: Ingresar a la herramienta Keepass, recientemente instalada.

- Buscar y seleccionar base de datos de credenciales: Consiste en buscar el archivo al que accede Keepass para buscar los accesos de la organización. Dicho archivo se encuentra en el repositorio organizacional de documentos.
- Solicitar clave de acceso a credenciales: Al seleccionar el archivo de credenciales, este solicita una contraseña, la cual se debe solicitar al mentor, en primera instancia.
- Solicitar clave a Líder de tribu: Si el mentor no conoce la clave de acceso a las credenciales, este debe solicitarla al líder de la tribu.
- Brindar clave de acceso a credenciales: el mentor, o líder de tribu debe brindar la contraseña de acceso a las credenciales. Esta debe darse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a “Credenciales.kdbx”: Se ingresa la clave brindada para poder entrar a la herramienta y acceder a los accesos y contraseñas.

Ilustración 29. Proceso Configuración Inicial



Fuente: Elaboración propia, 2022.

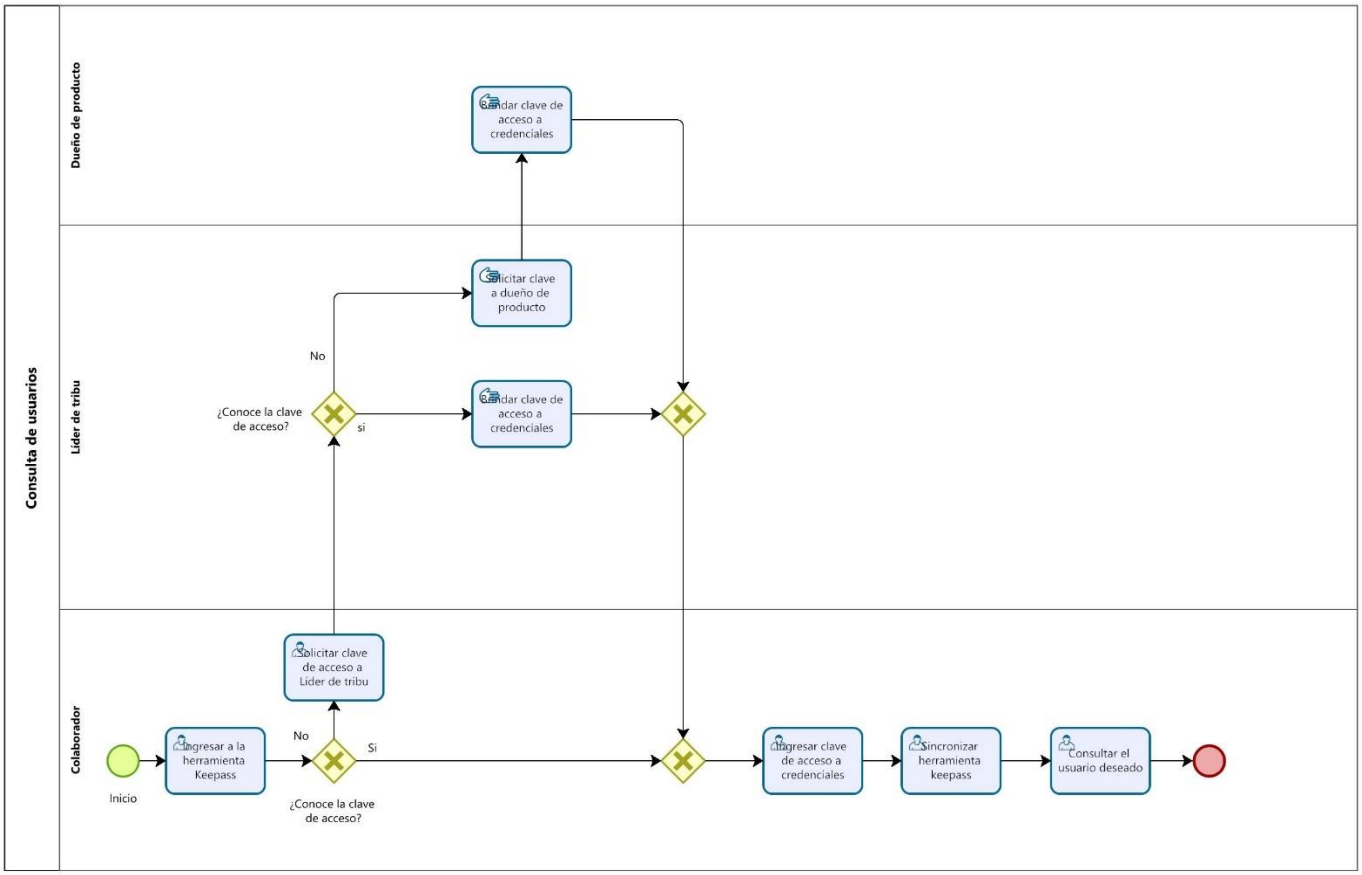
ati

5.2.1.2 Consulta de usuarios

El principal objetivo de este proceso es determinar el paso a paso para consultar sobre un acceso o contraseña en la herramienta Keepass, descrito en la sección 2.7.1 Keepass. En la Ilustración 30. Proceso Consulta de usuarios se puede visualizar el diagrama del proceso, el cual incluye las siguientes actividades:

- Ingresar a herramienta Keepass: Ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.
- Solicitar clave de acceso a líder de tribu: En caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- Solicitar clave a dueño de producto: Si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitarla al dueño de producto que corresponda.
- Brindar clave de acceso a credenciales: El dueño de producto, o líder de tribu debe brindar la contraseña de acceso a las credenciales. Esta debe darse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a credenciales: Se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- Sincronizar herramienta Keepass: Tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- Consultar el usuario deseado: Buscar entre los accesos y contraseñas existentes la que se necesite al momento la consulta.

Ilustración 30. Proceso Consulta de usuarios



Fuente: Elaboración propia, 2022.

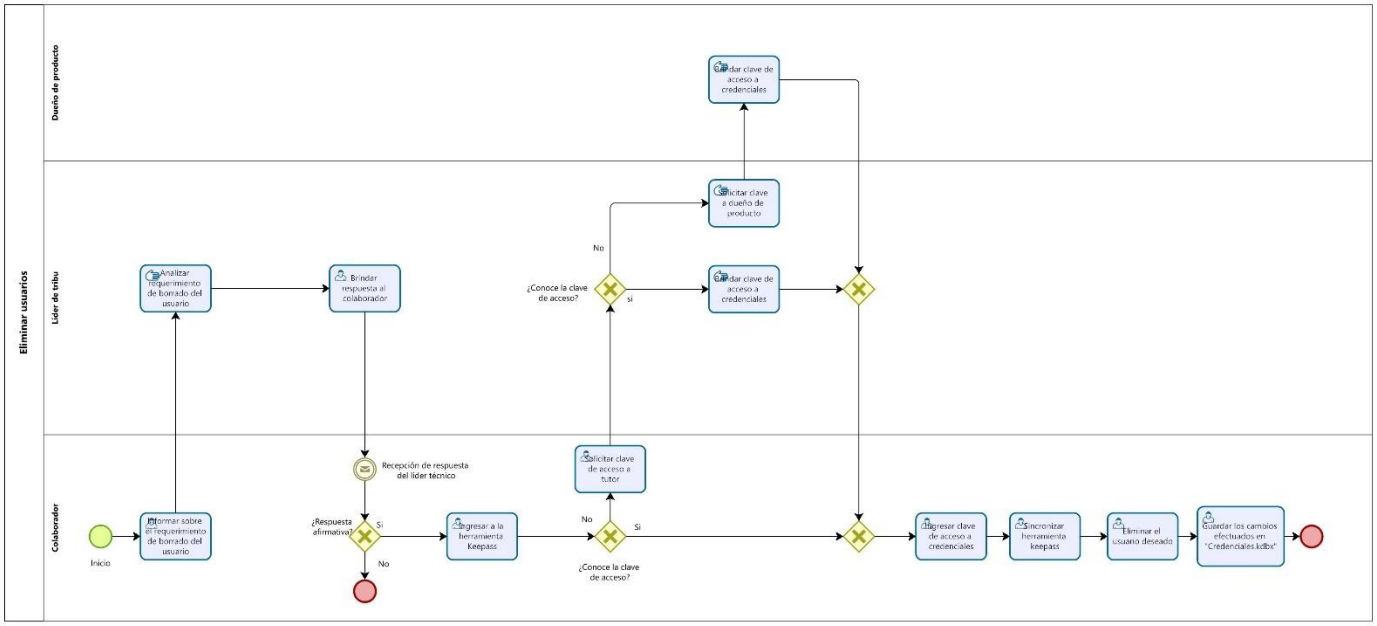
5.2.1.3 Eliminar usuarios

Proceso asociado a la política que se lleva a cabo para eliminar un usuario o acceso registrado en la herramienta Keepass, descrita en la sección 2.7.1 Keepass. En la Ilustración 31. Proceso Eliminar Usuarios, se muestra el proceso necesario para eliminar un usuario; incluye las siguientes actividades:

- Informar sobre el requerimiento de borrado del usuario: El colaborador debe informar al líder de tribu sobre el requerimiento y sus detalles.
- Analizar requerimiento de borrado del usuario: El líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesario eliminarlo o no.

- Brindar respuesta al colaborador: El líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.
- Ingresar a herramienta Keepass: Ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.
- Solicitar clave de acceso a Líder de tribu: En caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- Solicitar clave a dueño de producto: Si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitarla al dueño de producto que corresponda.
- Brindar clave de acceso a credenciales: El dueño de producto, o líder de tribu, debe brindar la contraseña de acceso a las credenciales. Esta debe darse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a credenciales: Se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- Sincronizar herramienta Keepass: Tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- Eliminar el usuario deseado: El colaborador busca y elimina el determinado usuario.
- Guardar los cambios efectuados en “Credenciales.kdbx”: El colaborador guarda los cambios en la herramienta, la cual actualiza el documento “Credenciales.kdbx”.

Ilustración 31. Proceso Eliminar Usuarios



Fuente: Elaboración propia, 2022.

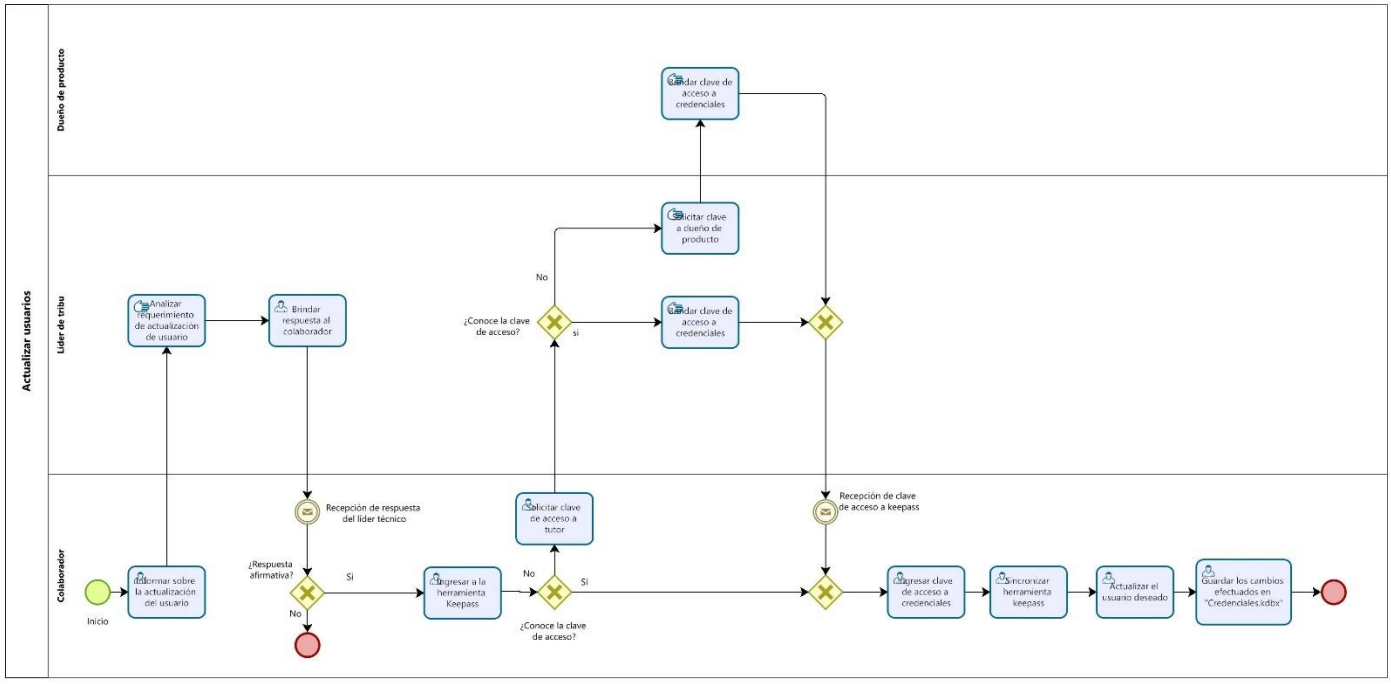
5.2.1.4 Actualizar usuarios

Este proceso contiene el conjunto de actividades necesarias para actualizar un acceso o usuario registrado en la herramienta Keepass. En la Ilustración 32. Proceso Actualizar usuarios, se encuentra el proceso necesario para llevar a cabo esta tarea, la cual incluye las siguientes actividades:

- Informar sobre la actualización del usuario: El colaborador debe informar al líder de tribu sobre el requerimiento y motivos por los cuales actualizar el usuario.
- Analizar requerimiento de actualización de usuario: El líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesaria la actualización.
- Brindar respuesta al colaborador: El líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.
- Ingresar a herramienta Keepass: Ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.

- Solicitar clave de acceso al líder de tribu: En caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- Solicitar clave a dueño de producto: Si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitarla al dueño de producto que corresponda.
- Brindar clave de acceso a credenciales: El dueño de producto, o líder de tribu, debe brindar la contraseña de acceso a las credenciales. Esta debe darse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a credenciales: Se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- Sincronizar herramienta Keepass: Tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- Actualizar el usuario deseado: El colaborador busca y actualiza el determinado usuario según lo que se requiera.
- Guardar los cambios efectuados en “Credenciales.kdbx”: El colaborador guarda los cambios en la herramienta, la cual actualiza el documento “Credenciales.kdbx”.

Ilustración 32. Proceso Actualizar usuarios



Fuente: Elaboración propia, 2022.

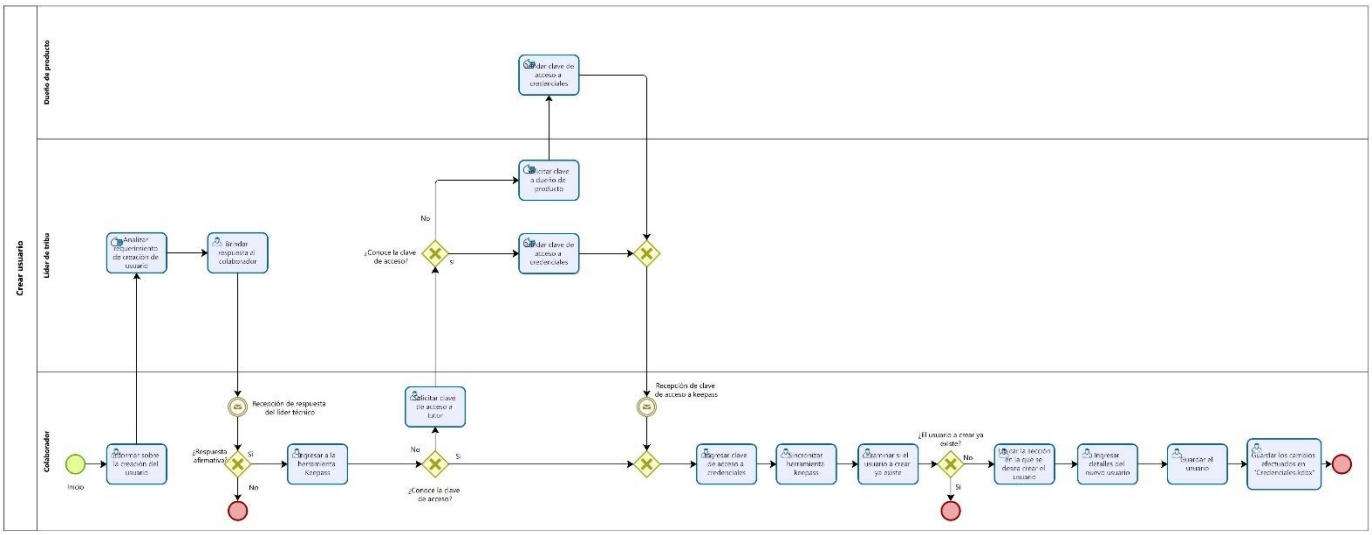
5.2.1.5 Crear Usuario

Proceso que se lleva a cabo para crear un usuario o acceso sobre la herramienta Keepass. En la Ilustración 33. Proceso Crear usuario, se evidencian las actividades que se deben llevar a cabo para cumplir con este proceso, estas son:

- Informar sobre la creación del usuario: El colaborador debe informar al líder de tribu sobre el requerimiento y motivos por los cuales crear el usuario.
- Analizar requerimiento de creación del usuario: El líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesaria la creación del usuario.
- Brindar respuesta al colaborador: El líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.
- Ingresar a herramienta Keepass: Esta se encuentra instalada en el equipo.
- Solicitar clave de acceso a líder de tribu: En caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- Solicitar clave a dueño de producto: Si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitarla al dueño de producto que corresponda.
- Brindar clave de acceso a credenciales: El dueño de producto, o líder de tribu, debe brindar la contraseña de acceso a las credenciales. Esta debe darse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a credenciales: Se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- Sincronizar herramienta Keepass: Tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- Examinar si el usuario a crear ya existe: El colaborador que desea crear el usuario revisa la herramienta Keepass para determinar si el usuario ya existe o no.
- Ubicar la sección en la que se desea crear el usuario: El colaborador revisa la estructura creada y determina en qué sección se debe crear el usuario.

- Ingresar detalles del nuevo usuario: El colaborador ingresa los detalles del usuario por crear, según corresponda.
- Guardar el usuario: Guardar en la herramienta los detalles del usuario creado.
- Guardar los cambios efectuados en “Credenciales.kdbx”: El colaborador guarda los cambios en la herramienta, la cual actualiza el documento “Credenciales.kdbx”.

Ilustración 33. Proceso Crear usuario



Fuente: Elaboración propia, 2022.

5.2.1.6 Revisión de usuarios

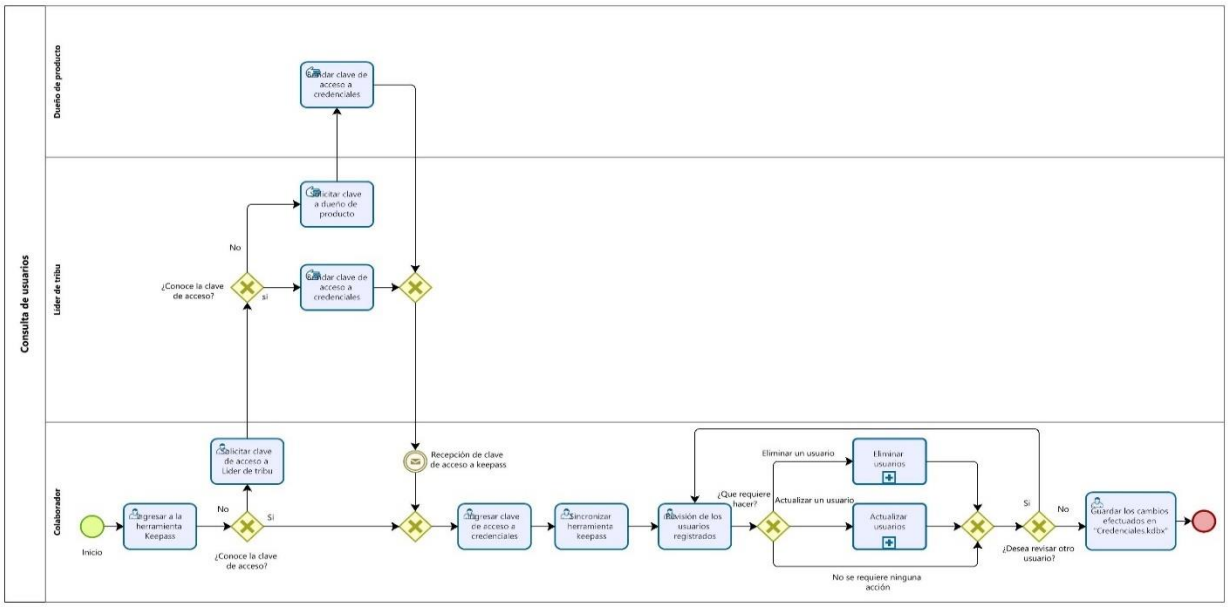
Este proceso se lleva a cabo con el objetivo de realizar una revisión sobre los usuarios existentes, con el fin de depurar la base de datos de accesos. En la Ilustración 34. Proceso Revisión de usuarios, se muestra el diagrama del proceso, así como las actividades que se deben llevar a cabo para su cumplimiento. Entre estas se encuentran:

- Ingresar a la herramienta Keepass: El colaborador ingresa a la herramienta Keepass, instalada en el equipo.
- Solicitar clave de acceso a Líder de tribu: En caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- Solicitar clave a dueño de producto: Si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitarla al dueño de producto que corresponda.

ati

- Brindar clave de acceso a credenciales: El dueño de producto, o líder de tribu, debe brindar la contraseña de acceso a las credenciales. Esta se otorga por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- Ingresar clave de acceso a credenciales: Se ingresa la clave brindada para entrar a la herramienta y visualizar los accesos y contraseñas.
- Sincronizar herramienta Keepass: Tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- Revisión de los usuarios registrados: El colaborador a cargo de la tarea revisa los usuarios existentes, para validar si se requiere eliminar o actualizar un usuario.
- Actualizar usuarios (subproceso): Si es requerido en la revisión, el usuario ejecuta el proceso de actualizar un usuario.
- Eliminar usuarios (subproceso): Si es requerido producto de la revisión, el usuario puede ejecutar el proceso de eliminar un usuario.
- Guardar los cambios efectuados en “Credenciales.kdbx”: El colaborador guarda los cambios en la herramienta, la cual actualiza el documento “Credenciales.kdbx”.

Ilustración 34. Proceso Revisión de usuarios



Fuente: Elaboración propia, 2022.

ati

5.2.2 Defensa contra software malicioso

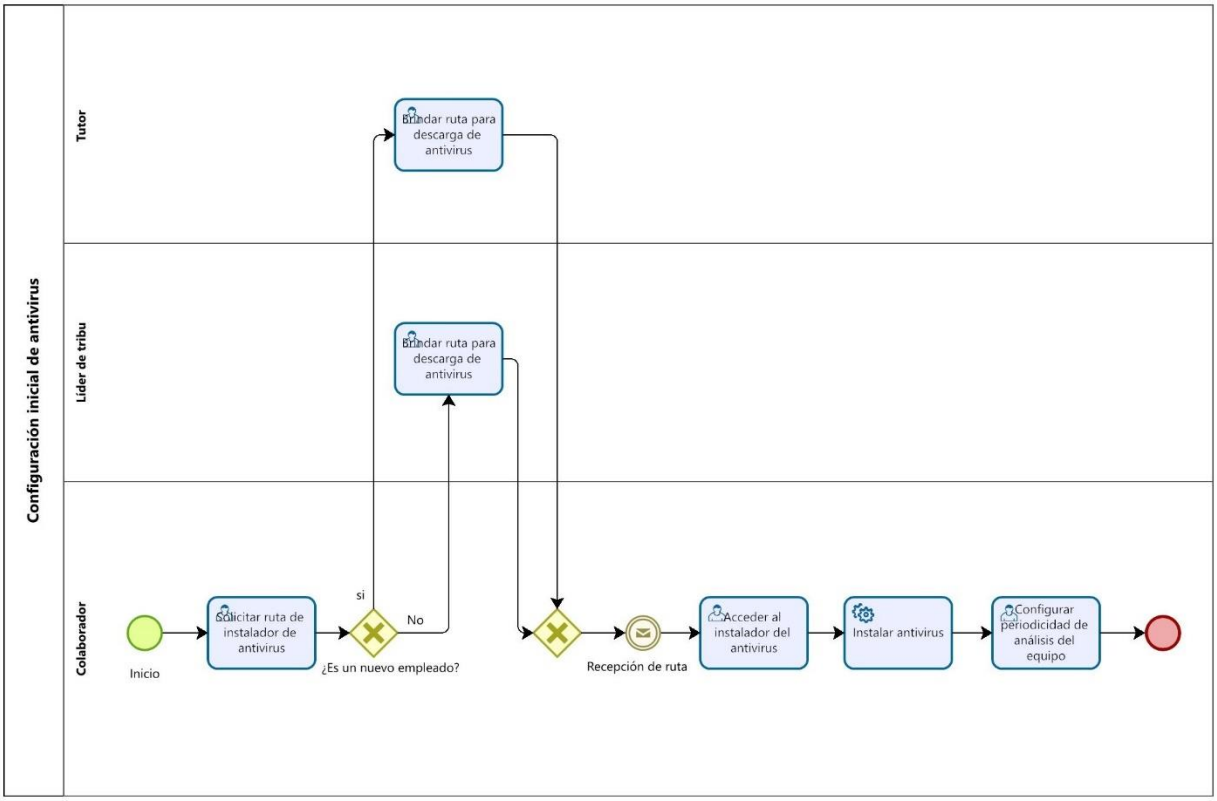
Para el desarrollo de esta política se tomaron como versión final los procesos expuestos en la Tabla 37. Procesos propuestos para política de defensa contra software malicioso. Estos procesos fueron definidos según la brecha identificada y detallada en la sección 5.1.1 Defensa contra software malicioso. Por tanto, el objetivo de esta sección es detallar, a nivel de actividad, cada uno de los diagramas *To-be* que soportan los procesos.

5.2.2.1 Configuración inicial de antivirus

Este proceso tiene como principal objetivo ser una guía de configuración para los colaboradores que deseen instalar en sus equipos el antivirus de la organización. En la Ilustración 35. Proceso Configuración inicial de antivirus, se muestra el diagrama del proceso, el cual cuenta con las siguientes actividades:

- Solicitar ruta de instalador de antivirus: El colaborador solicita la ruta de la cual debe descargar el instalador del antivirus.
- Brindar ruta para descarga de antivirus: El tutor o el líder de la tribu brinda la ruta de la cual el colaborador puede descargar el instalador del antivirus. Si se trata de un nuevo empleado, la ruta la brindará el mentor del nuevo colaborador, de lo contrario, deberá ser brindada por el líder de la tribu.
- Acceder al instalador de antivirus: El colaborador accede al instalador según la ruta que le fue brindada.
- Instalar antivirus: El colaborador ejecuta las acciones necesarias para que la instalación del antivirus sea efectiva.
- Configurar periodicidad de análisis del equipo: El colaborador configura qué tan seguido se hará la revisión automática del equipo.

Ilustración 35. Proceso Configuración inicial de antivirus



Fuente: Elaboración propia, 2022.

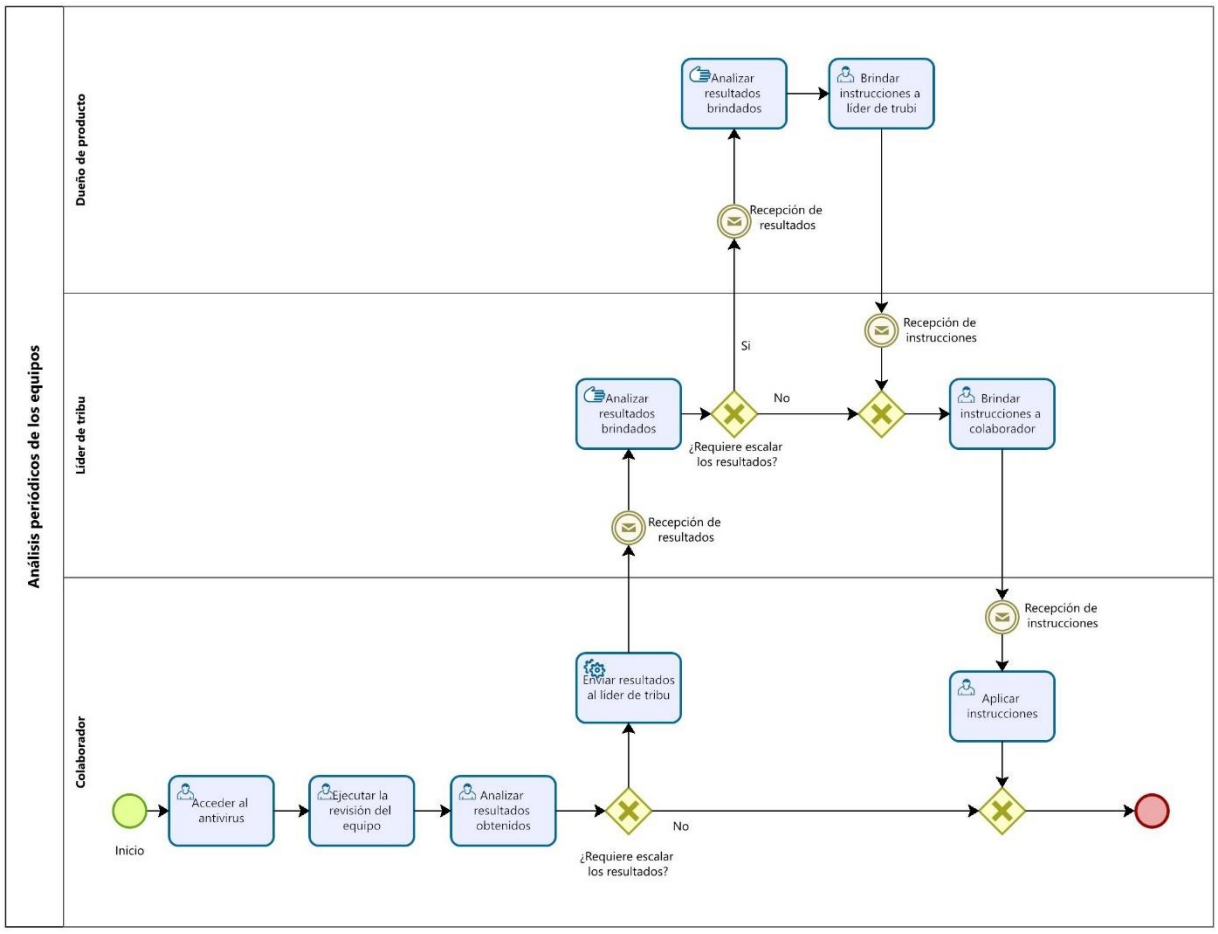
5.2.2.2 Análisis periódicos de los equipos

Este proceso menciona los pasos que el colaborador debe llevar a cabo cuando realice el análisis del equipo mediante el antivirus y según los resultados que este análisis arroje. En la Ilustración 36. Proceso Análisis periódicos de los equipos, se muestra el diagrama asociado al proceso mencionado. Este proceso cuenta con las siguientes actividades:

- Acceder al antivirus: El colaborador accede a la herramienta de antivirus instalada en su equipo.
- Ejecutar la revisión del equipo: El colaborador ejecuta la funcionalidad del antivirus que analiza el equipo y todos los archivos que en este se encuentran.

- Analizar resultados obtenidos: El colaborador analiza los resultados arrojados por la herramienta para determinar si estos requieren ser escalados o no.
- Enviar resultados al líder de tribu: El colaborador envía, de ser necesario, los resultados obtenidos para que el líder de tribu valide si ponen en riesgo información o equipos pertenecientes a la tribu.
- Analizar los resultados brindados: El líder de tribu, o el dueño de producto, evalúan los resultados aportados por el colaborador; esto para determinar las acciones correctivas por llevar a cabo.
- Brindar instrucciones a colaborador: El líder de tribu, o el dueño de producto, brindan realimentación al colaborador sobre las acciones por llevar a cabo.
- Aplicar instrucciones: El colaborador aplica las instrucciones brindadas por el líder de la tribu o por el dueño de producto.

Ilustración 36. Proceso Análisis periódicos de los equipos



Fuente: Elaboración propia, 2022.

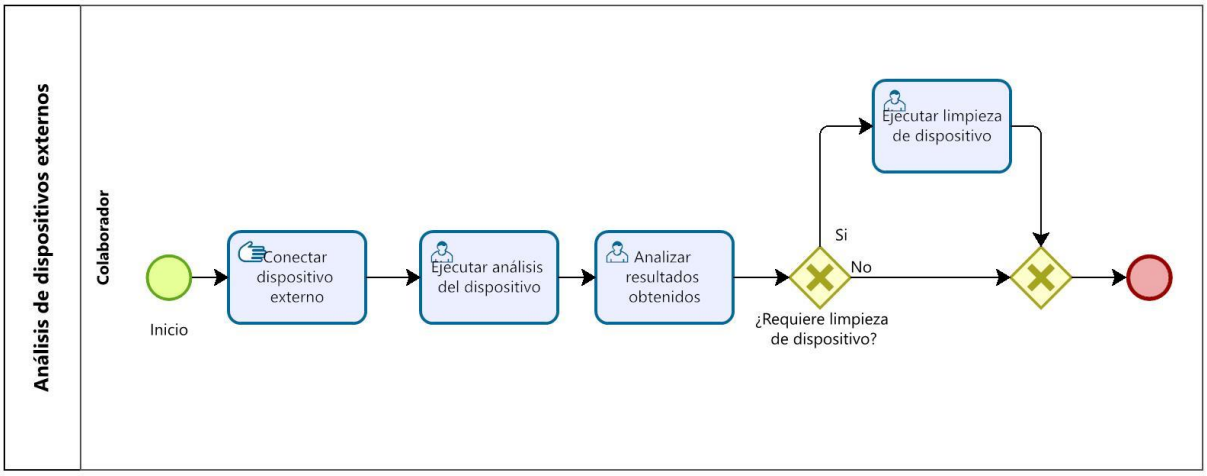
5.2.2.3 Análisis de dispositivos externos

Este proceso brinda el paso a paso que debe seguir un colaborador para ejecutar el análisis de algún dispositivo externo propio que conecte a un equipo de la organización. En la Ilustración 37. Proceso Análisis de dispositivos externos, se evidencia el diagrama asociado a dicho proceso, el cual contiene las siguientes actividades:

- Conectar dispositivo externo: El colaborador conecta al equipo el dispositivo externo.
- Ejecutar análisis del dispositivo: Antes de ingresar al dispositivo, el colaborador ejecuta el análisis de amenazas que provee el antivirus.

- Analizar resultados obtenidos: El colaborador analiza los resultados que arroja el antivirus, esto para determinar si es fiable ingresar o no.
- Ejecutar limpieza de dispositivo: De ser requerido, el colaborador se encargará de ejecutar la limpieza del dispositivo para eliminar cualquier tipo de amenazas.

Ilustración 37. Proceso Análisis de dispositivos externos



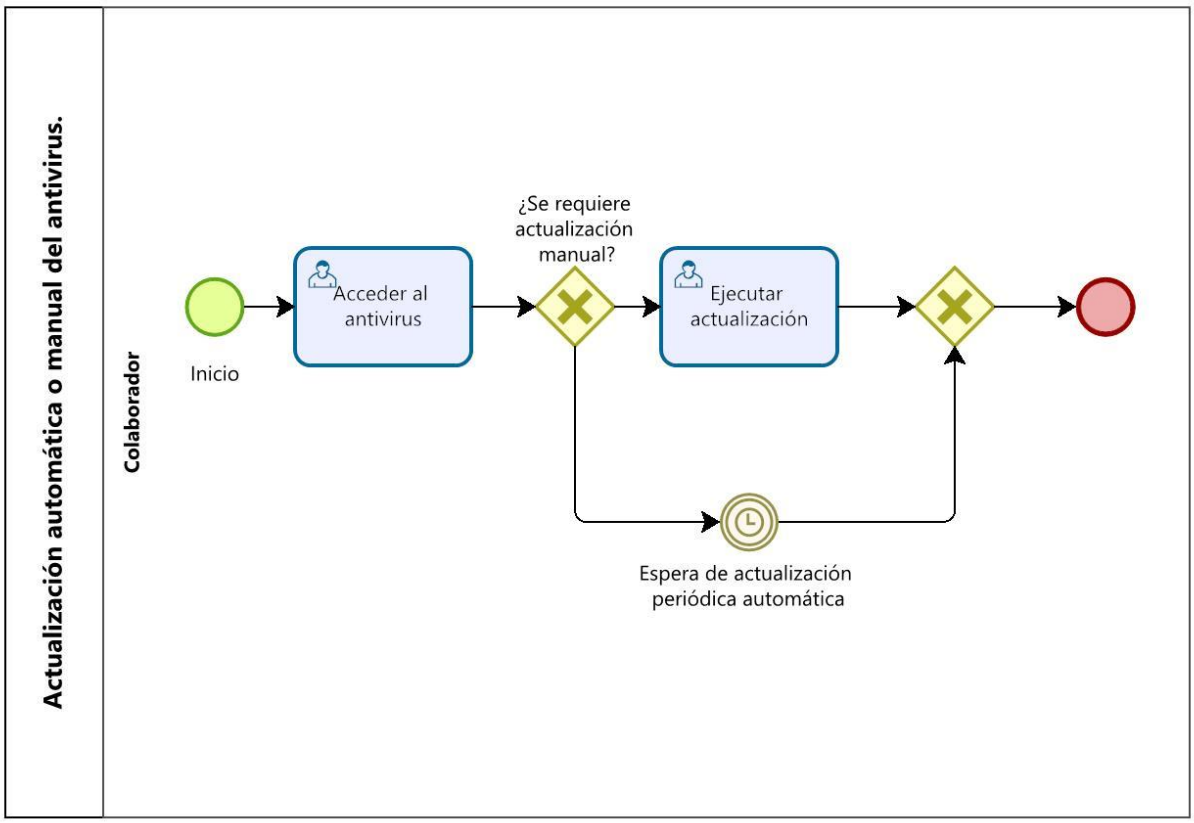
Fuente: Elaboración propia, 2022.

5.2.2.4 Actualización automática o manual del antivirus

Este proceso muestra las actividades necesarias para que el antivirus se actualice de forma manual o automática. En la Ilustración 38. Proceso Actualización automática o manual del antivirus, se puede visualizar el proceso de ejecución paso a paso, el cual cuenta con las siguientes actividades:

- Acceder al antivirus: El colaborador accede a la herramienta de antivirus instalada en su equipo.
- Ejecutar actualización: De ser requerido, el colaborador puede ejecutar la actualización manual del antivirus.

Ilustración 38. Proceso Actualización automática o manual del antivirus



Fuente: Elaboración propia, 2022.

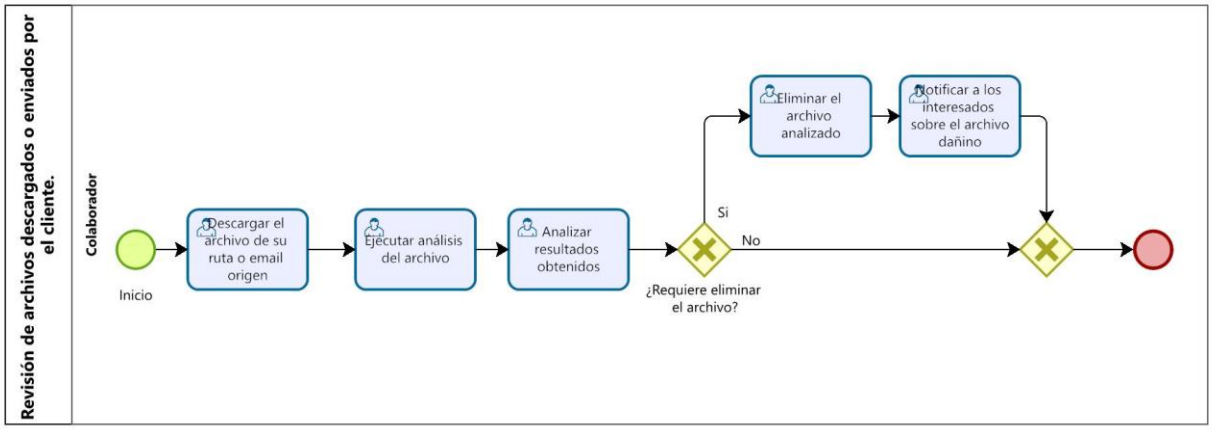
5.2.2.5 Revisión de archivos descargados o enviados por el cliente

Con el fin de evitar cualquier tipo de amenaza proveniente de archivos descargados de Internet o enviados por el cliente, este proceso muestra el paso a paso para analizar dichos archivos. En la Ilustración 39. Proceso Revisión de archivos descargados o enviados por el cliente, se incluye el diagrama del proceso. Este cuenta con las siguientes actividades:

- Descargar el archivo de su ruta o email origen: El colaborador descarga en el equipo el archivo que desea utilizar, ya sea de Internet o de la fuente aportada por el cliente.
- Ejecutar el análisis del archivo: Utilizando el antivirus, el colaborador ejecuta el análisis de los archivos descargados.
- Analizar resultados obtenidos: Según lo arrojado por el antivirus, el colaborador analiza dichos resultados obtenidos.

- Eliminar el archivo analizado: El colaborador borra del equipo el archivo analizado debido a algún riesgo arrojado por el antivirus.
- Notificar a los interesados sobre el archivo dañino: Se debe comunicar a los interesados de la organización sobre el borrado del archivo. Así mismo, se debe notificar al cliente, en caso de ser necesario, para que tome acciones preventivas.

Ilustración 39. Proceso Revisión de archivos descargados o enviados por el cliente



Fuente: Elaboración propia, 2022.

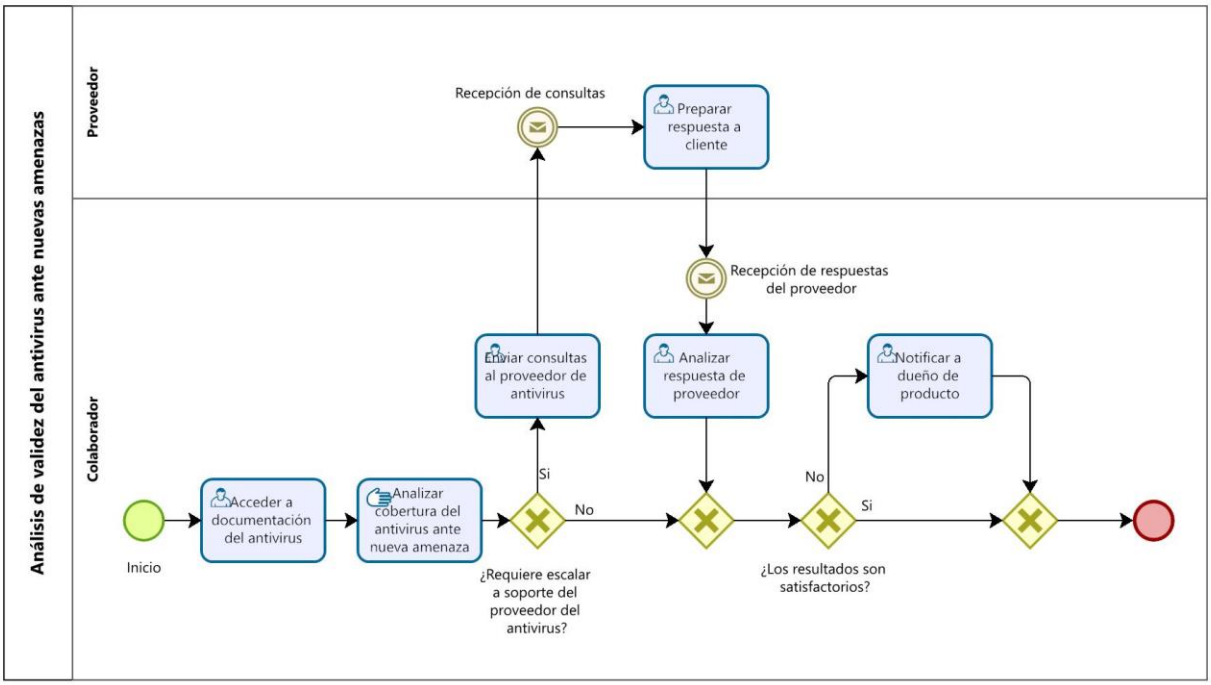
Análisis de validez del antivirus ante nuevas amenazas

Con el fin de determinar si el antivirus aún cubre a la organización contra nuevas amenazas, este proceso incluye todas las actividades necesarias para dicho análisis. En la Ilustración 40. Proceso Análisis de validez del antivirus ante nuevas amenazas, se muestra el diagrama asociado al proceso. Este diagrama incluye las siguientes actividades:

- Acceder a documentación del antivirus: El colaborador accede a la documentación aportada por el proveedor del antivirus.
- Analizar cobertura del antivirus ante nueva amenaza: El colaborador analiza si el antivirus ofrece protección a la organización sobre la nueva amenaza por investigar.
- Enviar consultas al proveedor de antivirus: El colaborador prepara y envía las consultas al proveedor del servicio, en caso de ser necesario.

- Preparar respuesta a cliente: El proveedor debe dar respuesta a las consultas de la organización.
- Analizar respuesta de proveedor: El colaborador analiza las respuestas aportadas por el proveedor y analiza si requiere escalarlo al dueño de producto necesario.
- Notificar a dueño de producto: De ser necesario, el colaborador puede escalar al dueño de producto la situación ocurrida con el antivirus.

Ilustración 40. Proceso Análisis de validez del antivirus ante nuevas amenazas



Fuente: Elaboración propia, 2022.

5.2.3 Inventario y control de los activos de software

Para el modelado *To-be* de esta política se tomaron como versión final los procesos expuestos en Tabla 39. Procesos propuestos para política de inventario y control de activos de software Además, estos fueron determinados según la brecha identificada en la sección 5.1.3 Inventario y control de los activos de software. En esta sección se detallan los procesos pertenecientes a esta política, así como los diagramas *To-be* pertenecientes a cada proceso.

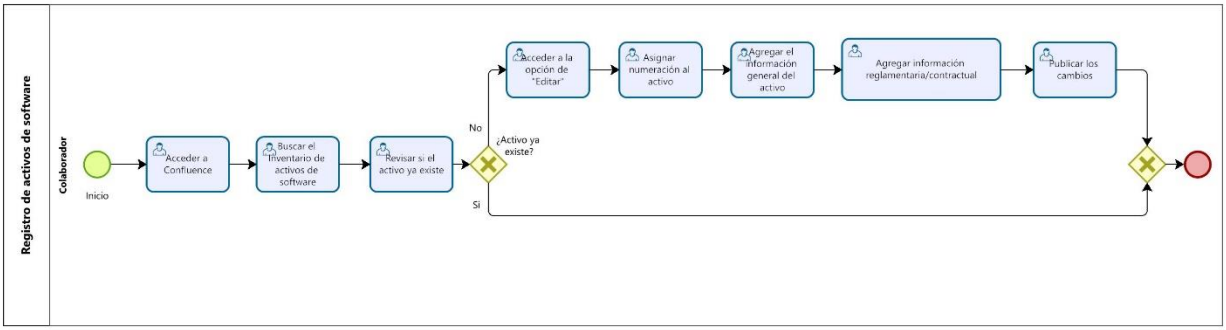
ati

5.2.3.1 Registro de activos de software

Este proceso tiene como finalidad brindar claridad sobre como registrar un activo de software sobre el inventario existente en la organización. Dicho inventario se encuentra en la herramienta Confluence, detallada en 2.7.2 Confluence, y la cual funciona como repositorio de conocimiento de la organización. En la Ilustración 41. Proceso Registro de activos de software, se muestra el diagrama asociado al proceso, el cual cuenta con las siguientes actividades:

- Acceder a Confluence: El colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- Buscar el inventario de activos de software: Al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- Revisar si el activo ya existe: El colaborador revisa y verifica que en el inventario no exista el activo de software por registrar.
- Acceder a la opción de “Editar”: Para poder editar el inventario, el colaborador debe acceder a la opción de “Editar”.
- Asignar numeración al activo: Al ingresar el activo, el colaborador revisa la numeración existente con el fin de asignar un número único.
- Agregar información reglamentaria/contractual: Agregar a la línea del activo la información reglamentaria y contractual que corresponda al activo de software.
- Publicar los cambios: Una vez ingresada toda la información relacionada al activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 41. Proceso Registro de activos de software



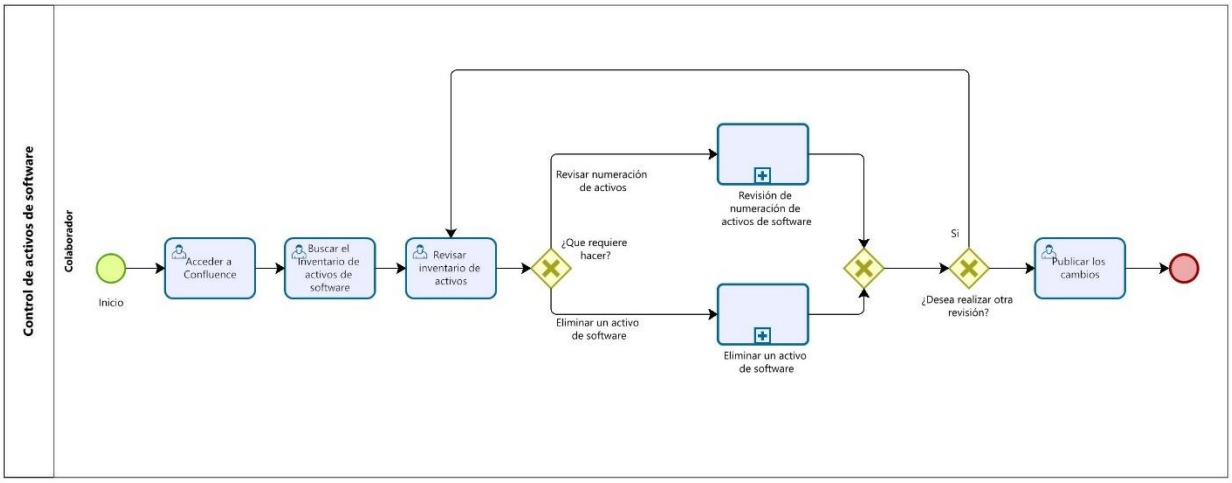
Fuente: Elaboración propia, 2022.

5.2.3.2 Control de activos de software

Este proceso tiene la finalidad de establecer revisiones sobre el inventario de activos de software para determinar si se requiere eliminar o enumerar alguno de los ya registrados. En la Ilustración 42. Proceso Control de activos de software, se muestra el diagrama asociado al proceso. Las actividades de este proceso son:

- Acceder a Confluence: El colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- Buscar el inventario de activos de software: Al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- Revisar inventario de activos: El colaborador revisa el inventario con el fin de determinar si se requiere actualizar alguno de los ya existentes.
- Revisión de numeración de activos de software (subproceso): Si fuera necesario, el colaborador puede ejecutar el proceso de numeración de activos de software producto de la revisión que haya realizado. Este proceso asigna numeración única a los activos de software.
- Eliminar un activo de software (subproceso): Si fuera necesario, el colaborador puede ejecutar el proceso de eliminar un activo de software; esto, producto de la revisión que haya realizado y de los resultados que haya obtenido.
- Publicar los cambios: Una vez ingresada toda la información relacionada con el activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 42. Proceso Control de activos de software



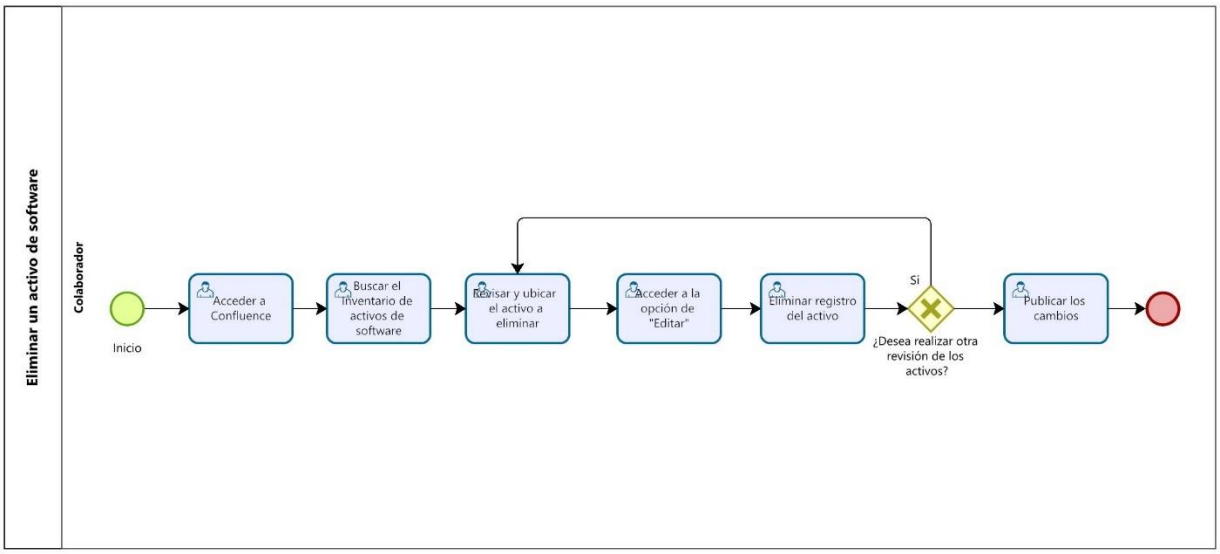
Fuente: Elaboración propia, 2022.

5.2.3.3 Eliminar un activo de software

Este proceso se lleva a cabo cuando sea necesario borrar un activo de software existente en el inventario. En la Ilustración 43. Proceso Eliminar un activo de software, se detalla el diagrama del proceso. Este cuenta con las siguientes actividades:

- Acceder a Confluence: El colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- Buscar el inventario de activos de software: Al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- Revisar y ubicar el activo a eliminar: Una vez ingresado en el inventario, el colaborador debe ubicar el activo por eliminar.
- Acceder a la opción de “Editar”: Para poder editar el inventario, el colaborador debe acceder a la opción de “Editar”.
- Eliminar el registro del activo: Al ubicarlo, el colaborador debe eliminar todos los datos asociados al activo de software.
- Publicar los cambios: Una vez ingresada toda la información relacionada con el activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 43. Proceso Eliminar un activo de software



Fuente: Elaboración propia, 2022.

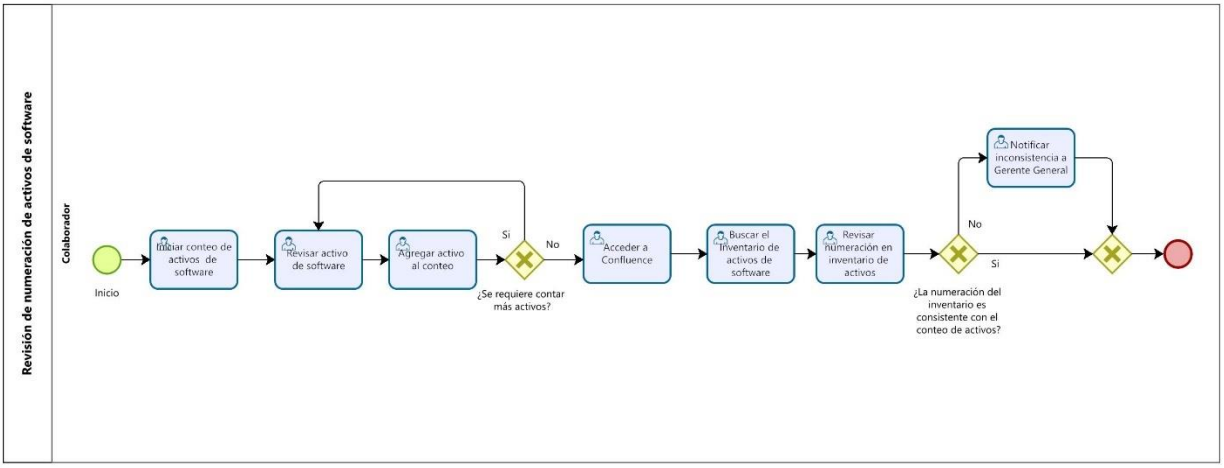
5.2.3.4 Revisión de numeración de activos de software

Este proceso tiene como objetivo asignar a cada activo de software un número de identificación específico, lo que permite ubicarlo a él y sus detalles contractuales y reglamentarios en el inventario. En la Ilustración 44. Proceso Revisión de numeración de activos de software, se detalla el proceso que se lleva a cabo para la enumeración, además, este proceso cuenta con las actividades:

- Iniciar conteo de activos de software: El colaborador revisa los activos de software y verifica que el número de activos existente corresponde a los registrados en el inventario.
- Revisar activo de software: El colaborador revisa que el activo de software por contar se encuentra en el inventario.
- Agregar activo al conteo: Si el conteo va bien, el colaborador agrega el activo de software al conteo del inventario.
- Acceder a Confluence: El colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.

- Buscar el inventario de activos de software: Al ingresar con sus credenciales, el colaborador debe buscar en *Confluence* el inventario de activos de software.
- Revisar numeración en inventario de activos: El colaborador revisa que la numeración realizada corresponda con la registrada en el inventario.
- Notificar inconsistencia al Gerente General: De ser necesario, el colaborador puede informar al Gerente General sobre alguna inconsistencia existente sobre el inventario de los activos de software.

Ilustración 44. Proceso Revisión de numeración de activos de software



Fuente: Elaboración propia, 2022.

5.3 Simulación de procesos

En esta sección se establecen las simulaciones necesarias para demostrar recursos y tiempos involucrados en las políticas que forman parte de la propuesta del presente proyecto. El objetivo de este apartado es establecer los insumos necesarios para determinar el costo financiero de la implementación de dichas políticas.

5.3.1 Defensa contra software malicioso

Según la identificación de la brecha entre la situación actual y el marco de referencia Cobit 5 descrita en la sección 5.1.1 Defensa contra software malicioso, se identifica que todos los procesos asociados a esta política son nuevos, por tanto, se puede asegurar que estos procesos no tienen una versión *As-Is* según la situación actual de la empresa.

El autor Zlaoui (2022) menciona que, los estudios de simulación son de interés cuando hay una falta de orientación en la literatura o cuando los métodos son novedosos. Según esto, los procesos asociados a esta política no son sujetos a estudios de simulación dado que cuentan con la guía del marco de referencia, además, no se pueden considerar como novedosos ya que, aunque sean nuevos en la empresa, si son implementados por muchas organizaciones en la actualidad. Esta premisa se determinó según la revisión documental detallada en Apéndice Q - Minuta RV 04 – 2208.

Por tanto, se puede definir que, si un proceso nuevo forma parte de una propuesta, no toma relevancia realizar simulación sobre el proceso propuesto, ya que los tiempos involucrados en dichos procesos no pueden ser calculados sobre la realidad de la empresa pues no han sido implementados

5.3.2 Control y uso de privilegios administrativos

Para la simulación de esta política su utilizó la herramienta Bizagi Modeler, descrita en la sección 2.7.3 Bizagi Modeler, la cual permite la construcción de procesos y dispone de las herramientas necesarias para simular un determinado proceso.

Relacionado a los tiempos *As-Is* de cada una de las tareas, en el Apéndice N - Minuta EM 07 – 2008 se establecen los tiempos mínimos y máximos de cada una de las tareas de los procesos *As-Is*.

Estos tiempos se obtuvieron mediante la realización de un grupo focal de diez personas pertenecientes a la organización y que habitualmente utilizan los procesos *As-is* que conforman esta política. Para la simulación de los procesos *To-Be,* en el Apéndice O - Minuta EM 08 – 2308 se definieron los tiempos de las actividades y procesos nuevos identificados en 5.1 Definición de la brecha relacionada con procesos existentes. Estos serán los tiempos utilizados para las simulaciones de cada una de las políticas expuestas en este apartado.

En cuanto a los costos de los recursos involucrados, se utilizará como base el salario mínimo establecido por el Ministerio de Trabajo de Costa Rica, el cual según MTSS es de ¢705.514,95 mensuales para el segundo semestre del 2022. A este monto, se le debe agregar el monto de cargas sociales, el cual corresponde a 26.5% sobre el total. Para determinar el monto final de salario, se debe realizar el siguiente cálculo:

¢705.514,95 * 1.265 = ¢892.476,42

En la Tabla 40. Salario Mínimo licenciatura Universitaria se muestra el detalle de los montos utilizados como salario base.

Tabla 40. Salario Mínimo licenciatura Universitaria

Salario mínimo licenciatura universitaria	
Mensual	¢892.476,42
Diario	¢44.623,82
Hora	¢5577,98

Fuente: Elaboración propia, 2022

Si bien los tiempos son de vital importancia para que las simulaciones de los procesos se acerquen lo más posible a implementaciones reales, para efectos de este proyecto no se realizará análisis de los tiempos arrojados por la simulación; esto, debido a que la naturaleza de este proyecto es la propuesta de políticas de seguridad que promuevan la estandarización de los procesos basados en COBIT 5 como marco de referencia, por tanto, las simulaciones deben ir orientadas al costo de aplicar las políticas estandarizadas y no a factores de tiempos.

La distribución de probabilidad utilizada para la simulación de los procesos de esta política es la denominada *distribución normal.* Se utiliza esta distribución debido al teorema central del límite, el cual, según Abarca (s.f), establece que dada muestra grande de una determinada población seguirá una distribución normal. En el caso de esta investigación y según se establece en el Apéndice N - Minuta EM 07 – 2008, las diez personas participantes del grupo focal se consideran una muestra grande, ya que el total de personas que utilizan la política en la organización asciende a cuarenta, por tanto, la muestra corresponde a un 25% de la población total. Para la simulación de los procesos *As-Is* y *To-be* se asume normalidad.

5.3.2.1 Proceso: Configuración inicial

A continuación, se detallan los resultados obtenidos de la simulación de los procesos *As-Is* y de los procesos *To-be.*

5.3.2.1.1 Proceso *As-Is*

Según los tiempos obtenidos mediante el grupo focal para las actividades del proceso *As-Is 4.4.2.1* Configuración inicial, los cuales se detallan en el Apéndice N - Minuta EM 07 – 2008, se aplica la distribución normal y se obtiene como resultado los promedios y medias por actividad expuestos en la Tabla 41. Tiempos As-Is Configuración Inicial.

Tabla 41. Tiempos As-Is Configuración Inicial

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Descargar la herramienta Keepass	1	5	3	2
Instalar la herramienta Keepass	2	3	2,5	0,5
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Buscar y seleccionar base de datos de credenciales	10	15	12,5	2,5
Solicitar clave de acceso a credenciales	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a "Credenciales.kdbx"	0,5	1	0,75	0,25

Fuente: Elaboración propia, 2022.

Tomando los datos de la Tabla 41. Tiempos As-Is Configuración Inicial y aplicándolos a la simulación de recursos, se obtienen los resultados expuestos en la Tabla 42. Simulación recursos Configuración Inicial As-Is.

Tabla 42. Simulación recursos Configuración Inicial As-Is

Recurso	Uso	Costo unitario total	Costo total
Consultor 3	1.41 %	14517.2940889967	14517.2940889967
Consultor 1	100.00 %	6845474.68963125	6845474.68963125
Consultor 2	1.43 %	73366.6093655406	73366.6093655406
Total		6933358.69	6933358.69

Fuente: Elaboración propia, 2022.

Según los datos de la Tabla 42. Simulación recursos Configuración Inicial As-Is, se definieron los recursos de la siguiente manera:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el mentor del colaborador.
- Consultor 3: Se refiere a las tareas ejecutadas por el líder de tribu.

Por tanto, según los recursos detallados previamente y las actividades que forman parte del proceso *4.4.2.1* Configuración inicial, la simulación arroja que el proceso tiene un costo total de ¢6.933.358,69 para un número total de cuarenta ejecuciones. En la Tabla 43. Simulación tiempo Configuración Inicial As-Is, se evidencia el tiempo total y unitario de cada tarea arrojado por la simulación, que conllevan al costo mostrado en la Tabla 42. Simulación recursos Configuración Inicial As-Is.

Tabla 43. Simulación tiempo Configuración Inicial As-Is

Nombre	Tipo	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Inicio	Evento de inicio			
Descargar la herramienta Keepass	Tarea	3.70391104823625	124.12135944225	2564.18341432244
Instalar herramienta Keepass	Tarea	24.1156344696921	125.670350094496	4071.0755846632
Buscar y seleccionar base de datos de credenciales	Tarea	93.2847892136409	663.412522344536	14324.4968259917
Solicitar clave de acceso a credenciales	Tarea	167.878122055308	1317.04015134835	36721.4867173917
¿Conoce la clave de acceso?	Compuerta			
Brindar clave de acceso a credenciales	Tarea	1.04141536028624	1.89399737132851	25.718345859994
Solicitar clave a dueño de producto	Tarea	21.9353889475979	57.7437311155227	972.586793291068
Brindar clave de acceso a credenciales	Tarea	1.02886553632675	1.86938825386528	32.9229909467504
ExclusiveGateway	Compuerta			
Ingresar clave de acceso a "Credenciales.kdbx"	Tarea	25.7612530358824	1313.76082151742	26769.3716169706
Ingresar a herramienta Keepass	Tarea	81.3916948363925	123.393589961859	3655.03045057421
Final	Evento de Fin			
Configuración inicial (Total)	Proceso	1065.22219160067	2309.17261472396	89136.8727400117

Fuente: Elaboración propia, 2022.

5.3.2.1.2 Proceso *To-be*

Según se indica en el Apéndice O - Minuta EM 08 – 2308 y basado en la brecha identificada para el proceso en la sección 5.1.2 Control y uso de privilegios administrativos, se determina que los tiempos y actividades del proceso son los mismos de su versión *As-Is.* Siendo así, se pueden tomar los resultados de la simulación del proceso *As-Is* como los resultados de la versión *To-be.* Por tanto, los resultados de la simulación de costos para este proceso arrojan un total de ¢6.933.358,69.

5.3.2.2 *Proceso: Crear Usuario*

En esta sección se detallan los aspectos relacionados con las simulaciones realizadas al proceso *As-Is* y el proceso *To-be.*

5.3.2.2.1 Proceso *As-Is*

Tomando como referencia los tiempos obtenidos del grupo focal mencionado en el Apéndice N - Minuta EM 07 – 2008 para cada una de las actividades descritas en el proceso 4.4.2.5

Creación de usuario, se aplica la distribución normal. Se obtuvieron como resultado los promedios y medias por actividad expuestos en la Tabla 44. Tiempos As-Is Crear Usuario.

Tabla 44. Tiempos As-Is Crear Usuario

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Ingresar a herramienta Keepass	0,25	1	0,625	0,5303301
Solicitar clave de acceso a líder de tribu	20	60	40	28,284271
Solicitar clave a dueño de producto	20	60	40	28,284271
Brindar clave de acceso a credenciales	1	2	1,5	0,7071068
Brindar clave de acceso a credenciales	1	2	1,5	0,7071068
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,3535534
Sincronizar herramienta keepass	0,5	1	0,75	0,3535534
Ubicar la sección en la que se desea crear el usuario	1	2	1,5	0,7071068
Ingresar nombre de usuario	1	3	2	1,4142136
Ingresar contraseña	1	3	2	1,4142136
Ingresar enlace del ambiente	1	3	2	1,4142136
Guardar el usuario	0,25	1	0,625	0,5303301
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,3535534

Fuente: Elaboración propia, 2022.

Si se toman como base los tiempos detallados en la Tabla 44. Tiempos As-Is Crear Usuario y se realiza la simulación de recursos, se pueden visualizar los costos que se muestran en la Tabla 45. Simulación recursos Crear Usuario As-Is.

Tabla 45. Simulación recursos Crear Usuario As-Is

Recurso	Uso	Costo unitario total	Costo total
Consultor 3	0.83 %	7442.6924222892	7442.6924222892
Consultor 1	94.25 %	5657835.84435201	5657835.84435201
Consultor 2	1.08 %	48436.6499166445	48436.6499166445
Total		5713715.19	5713715.19

Fuente: Elaboración propia, 2022.

Según los datos de la Tabla 45. Simulación recursos Crear Usuario As-Is, se definieron los recursos participantes del proceso de la siguiente manera:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el mentor del colaborador.
- Consultor 3: Se refiere a las tareas ejecutadas por el líder de tribu.

En conclusión, según los recursos detallados previamente y las actividades que forman parte del proceso 4.4.2.5 Creación de usuario, la simulación arroja que el proceso tiene un costo total de ¢5.713.715,69, para un número total de cuarenta ejecuciones. En la Tabla 46. Simulación tiempo Crear Usuario As-Is, se evidencia el tiempo total y unitario de cada tarea arrojados por la simulación y que conducen al costo mostrado en la Tabla 45. Simulación recursos Crear Usuario As-Is.

Tabla 46. Simulación tiempo Crear Usuario As-Is

Nombre	Tipo	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Inicio	Evento de inicio			
Ingresar a la herramienta Keepass	Tarea	0.807222847773175	27.2714201699997	570.816384027245
¿Conoce la clave de acceso?	Compuerta			
Brindar clave de acceso a credenciales	Tarea	1.0959909741066	1.96972332516384	21.9693749664447
Solicitar clave a dueño de producto	Tarea	653.856031006786	1153.66817452293	11454.5780510311
Brindar clave de acceso a credenciales	Tarea	1.13669700163382	1.89960784501409	16.8788820930615
Guardar el usuario	Tarea	22.7750200644762	82.005711391362	2109.30914523417
¿Conoce la clave de acceso?	Compuerta			
Solicitar clave de acceso a tutor	Tarea	56.1926346863451	1139.73890573385	16430.7057827154
ExclusiveGateway	Compuerta			
ExclusiveGateway	Compuerta			
Ingresar clave de acceso a credenciales	Tarea	27.2536942222923	1139.86436343744	23453.7335314516
NoneEnd	Evento de Fin			
Sincronizar herramienta keepass	Tarea	35.0012949382467	1139.75183852987	13386.9586446093
Guardar los cambios efectuados en "Credenciales.kdbx"	Tarea	11.4306501213484	63.1831225930155	1327.71037552084
Ubicar la sección en la que se desea crear el usuario	Tarea	34.7910286398494	491.511190257704	3729.55192264251
Ingresar nombre de usuario	Tarea	37.9493272394816	80.1896681772644	2532.48439023804
Ingresar contraseña	Tarea	55.0076556945271	83.6298995872419	2955.98420136878
Ingresar enlace del ambiente	Tarea	46.6327855147276	82.8631316735889	2775.60929314685
Crear usuario	Proceso	1970.58995580604	2042.10965350147	80766.2899790454

Fuente: Elaboración propia, 2022.

5.3.2.2.2 Proceso *To-be*

Si se toman como base los tiempos obtenidos según lo descrito en el Apéndice O - Minuta EM 08 – 2308 para cada una de las actividades descritas en el proceso 5.2.1.5 Crear Usuario, se aplica la distribución normal; se obtienen como resultado los promedios y medias por actividad expuestos en la Tabla 44. Tiempos As-Is Crear Usuario.

Tabla 47. Tiempos To-be Crear Usuario

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Informar sobre el requerimiento de borrado del usuario	2	5	3,5	1,5
Analizar requerimiento de borrado del usuario	2	5	3,5	1,5
Brindar respuesta al colaborador	2	5	3,5	1,5
Ingresar a herramienta Keepass	0,25	1	0,625	0,5303301
Solicitar clave de acceso a líder de tribu	20	60	40	28,284271
Solicitar clave a dueño de producto	20	60	40	28,284271
Brindar clave de acceso a credenciales	1	2	1,5	0,7071068
Brindar clave de acceso a credenciales	1	2	1,5	0,7071068
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,3535534
Sincronizar herramienta keepass	0,5	1	0,75	0,3535534
Examinar si el usuario a crear ya existe	1	2	1,5	0,7071068
Ubicar la sección en la que se desea crear el usuario	1	2	1,5	0,7071068
Ingresar detalles del nuevo usuario	1	3	2	1,4142136
Guardar el usuario	0,25	1	0,625	0,5303301
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,3535534

Fuente: Elaboración propia, 2022.

Al tomar como referencia los tiempos detallados en la Tabla 47. Tiempos To-be Crear Usuario para realizar la simulación de recursos, se obtienen como resultado los costos determinados en la Tabla 48. Simulación recursos Crear Usuario To-be.

Tabla 48. Simulación recursos Crear Usuario To-be

Recurso	Uso	Costo unitario total	Costo total
Consultor 1	100.00 %	1234467.05004906	1234467.05004906
Consultor 2	77.38 %	143291.14276078	143291.14276078
Consultor 3	0.35 %	321.462647222039	321.462647222039
Total		1378079.66	1378079.66

Fuente: Elaboración propia, 2022.

Según los recursos mostrados en la Tabla 48. Simulación recursos Crear Usuario To-be, estos se definieron de la siguiente forma:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de Colaborador
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu a la que pertenece el colaborador.
- Consultor 3: Se refiere a las tareas ejecutadas por un determinado dueño de producto.

Por tanto, según los recursos detallados previamente y las actividades que forman parte del proceso 5.2.1.5 Crear Usuario, la simulación arroja que el proceso tiene un costo total de ¢1.378.079,66 para un número total de cuarenta ejecuciones. En la Tabla 49. Simulación tiempo Crear Usuario To-be, se evidencia el tiempo total y unitario de cada tarea, arrojados por la simulación y que conducen al costo mostrado en la Tabla 48. Simulación recursos Crear Usuario To-be.

Tabla 49. Simulación tiempo Crear Usuario To-be

Nombre	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Inicio			
Ingresar a la herramienta Keepass	3.62525213051231	105.416010444766	516.303586584495
¿Conoce la clave de acceso?			
Brindar clave de acceso a credenciales	1.48850023952099	73.124130674437	191.539566722052
Solicitar clave a dueño de producto	39.5199951704463	39.5199951704463	39.5199951704463
Brindar clave de acceso a credenciales	1.45821114639165	1.45821114639165	1.45821114639165
Guardar el usuario	1.96317119249704	69.93670787016	101.136581985643
¿Conoce la clave de acceso?			
Solicitar clave de acceso a tutor	31.8092075711743	103.866703038187	356.819492758189
Ingresar clave de acceso a credenciales	4.40625040784749	103.540490989054	704.073620650435
NoneEnd			
Sincronizar herramienta keepass	2.87025979904638	103.701893005451	352.892438671563
Guardar los cambios efectuados en "Credenciales.kdbx"	1.45302458984736	11.9418666884624	34.1430109876358
Ubicar la sección en la que se desea crear el usuario	5.53270784554832	107.702899651975	185.932883377091
Ingresar detalles del nuevo usuario	3.30237685871231	49.2565818769643	88.6842609247375
Informar sobre la creación del usuario	4.11363314336071	103.055229822782	2042.49116355276
Analizar requerimiento de creación de usuario	4.64511056422386	88.0927524428282	1876.14714788482
Brindar respuesta al colaborador	8.6171164553846	88.1125902068325	2302.43812796324
¿Respuesta afirmativa?			
Recepción de respuesta del líder técnico			
Recepción de clave de acceso a keepass			
Examinar si el usuario a crear ya existe	5.3956752651294	107.100242435657	526.316218210562
¿El usuario a crear ya existe?			
Crear usuario	24.7826454206536	404.745126990746	9319.89630659007

Fuente: Elaboración propia, 2022

5.3.2.3 Proceso: Consulta de usuarios

En este apartado se detalla la simulación realizada al proceso *As-Is* y al proceso *To-Be.*

5.3.2.3.1 Proceso *As-Is*

Para la obtención de los tiempos de las actividades del proceso 4.4.2.2Consulta de usuarios, se preguntó a diez colaboradores de la organización los tiempos mínimos y máximos, mediante un grupo focal. Este ejercicio se evidencia en la Minuta XX.

Para la simulación de este proceso se usan los tiempos que se presentan en la Tabla 50. Tiempos As-Is Consulta de usuarios.

Tabla 50. Tiempos As-Is Consulta de usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Solicitar clave de acceso a líder de tribu	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,25
Sincronizar herramienta keepass	0,5	1	0,75	0,25
Consultar el usuario deseado	2	5	3,5	1,5

Fuente: Elaboración propia, 2022

Tomando los tiempos de la Tabla 50. Tiempos As-Is Consulta de usuarios como insumo para realizar la simulación de recursos y obtener los costos de la aplicación del proceso 4.4.2.2Consulta de usuarios, se obtiene como resultado el costo total detallado en la Tabla 51. Simulación recursos Consulta de usuarios As Is.

Tabla 51. Simulación recursos Consulta de usuarios As Is

Recurso	Uso	Costo unitario total	Costo total
Consultor 3	1.20 %	2358.48835804889	2358.48835804889
Consultor 1	96.06 %	2524571.52274186	2524571.52274186
Consultor 2	35.50 %	139938.384056488	139938.384056488
Total		2666868.4	2666868.4

Fuente: Elaboración propia, 2022.

Según los datos de la Tabla 51. Simulación recursos Consulta de usuarios As Is, se definieron los siguientes recursos como participantes del proceso:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

Por tanto, los recursos detallados anteriormente y las actividades y sus tiempos, que forman parte del proceso 4.4.2.2Consulta de usuarios, la simulación arroja que el proceso tiene un costo total de ¢2.666.868,69 para un número total de cuarenta ejecuciones. En la Tabla 52. Simulación tiempo Consulta de usuarios As-Is se evidencia el tiempo total y unitario de cada tarea, arrojados por la simulación y que conducen al costo mostrado en la Tabla 51. Simulación recursos Consulta de usuarios As Is.

Tabla 52. Simulación tiempo Consulta de usuarios As-Is

Nombre	Tipo	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Inicio	Evento de inicio			
Ingresar a la herramienta Keepass	Tarea	0.770524988210964	27.495667529635	574.461404047361
¿Conoce la clave de acceso?	Compuerta			
Brindar clave de acceso a credenciales	Tarea	1.08196498892607	22.7599222660974	52.3854436425681
Solicitar clave a dueño de producto	Tarea	26.5465440921733	56.9284851281285	303.723984706372
Brindar clave de acceso a credenciales	Tarea	1.02150959170365	1.97550728750574	10.6985182946196
Consultar el usuario deseado	Tarea	17.4362018038577	86.206961119079	2197.47022831652
¿Conoce la clave de acceso?	Compuerta			
Solicitar clave de acceso a tutor	Tarea	59.9685394450328	711.456607440575	6468.87228978539
ExclusiveGateway	Compuerta			
ExclusiveGateway	Compuerta			
Ingresar clave de acceso a credenciales	Tarea	27.7001802128729	618.895422690291	12501.4350573693
NoneEnd	Evento de Fin			
Sincronizar herramienta keepass	Tarea	26.2136593481605	710.498236435793	10868.2716694527
Consulta de usuarios	Proceso	756.405143440735	894.139365411611	32977.3185956148

Fuente: Elaboración propia, 2022.

5.3.2.3.2 Proceso To-be

Según la información recopilada en el Apéndice O - Minuta EM 08 – 2308 y tomando como base la brecha identificada para este proceso en la sección 5.1.2 Control y uso de privilegios administrativos, se determina que los tiempos y actividades del proceso *To-be* son los mismos de su versión *As-Is.* Siendo así, se pueden tomar los resultados de la simulación del proceso *As-Is* como los resultados de la versión *To-be.* Por tanto, los resultados de la simulación de costos para este proceso arrojan un total de ¢2.666.868,4.

5.3.2.4 Proceso: Eliminar Usuarios

A continuación, se detallan los resultados obtenidos de las simulaciones aplicadas a los procesos *As-Is* y *To-be*

5.3.2.4.1 Proceso *As-Is*

Para la recopilación de los tiempos relacionados con las actividades del proceso 4.4.2.3 Eliminar usuarios, se realizó un ejercicio en conjunto con diez colaboradores de la organización para obtener los tiempos mínimos y máximos. Mediante este ejercicio se evidencia en el Apéndice

N - Minuta EM 07 – 2008. Para la simulación de este proceso se usan los tiempos que se presentan en la Tabla 53. Tiempos As-Is Eliminar Usuarios, los cuales son el resultado del grupo focal demostrado en el Apéndice N - Minuta EM 07 – 2008.

Tabla 53. Tiempos As-Is Eliminar Usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Solicitar clave de acceso a líder de tribu	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,25
Sincronizar herramienta keepass	0,5	1	0,75	0,25
Eliminar el usuario deseado	2	5	3,5	1,5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,25

Fuente: Elaboración propia, 2022.

Al ejecutar la simulación del proceso 4.4.2.3 Eliminar usuarios, tomando como base los tiempos de la Tabla 53. Tiempos As-Is Eliminar Usuarios, se obtienen los costos detallados en la Tabla 54. Simulación recursos Eliminar usuarios As Is.

Tabla 54. Simulación recursos Eliminar usuarios As Is

Recurso	Uso	Costo unitario total	Costo total
Consultor 3	1.99 %	5146.12177402343	5146.12177402343
Consultor 1	96.99 %	3338377.22223522	3338377.22223522
Consultor 2	56.60 %	292217.77869121	292217.77869121
Total		3635741.12	3635741.12

Fuente: Elaboración propia, 2022.

En relación con los datos de la Tabla 54. Simulación recursos Eliminar usuarios As Is, se definieron los siguientes recursos participantes:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

Por tanto, si se toman los recursos detallados anteriormente, las actividades y sus tiempos, que en conjunto forman el proceso 4.4.2.3 Eliminar usuarios, la simulación concluye con que el proceso tiene un costo total de ¢3.635.741,12 para un número total de cuarenta ejecuciones. En la Tabla 52. Simulación tiempo Consulta de usuarios As-Is se evidencia el tiempo total y unitario de cada tarea, arrojados por la simulación y que conducen al costo mostrado en la Tabla 51. Simulación recursos Consulta de usuarios As Is.

Tabla 55. Simulación tiempo Eliminar Usuarios As-Is

Nombre	Tipo	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Inicio	Evento de inicio			
Ingresar a la herramienta Keepass	Tarea	0.770524988210964	27.495667529635	574.461404047361
¿Conoce la clave de acceso?	Compuerta			
Brindar clave de acceso a credenciales	Tarea	1.08196498892607	51.0307285279874	100.899661666038
Solicitar clave a dueño de producto	Tarea	28.5920431661541	76.2102472411444	723.410917427209
Brindar clave de acceso a credenciales	Tarea	1.02150959170359	1.99826164632952	23.3437141030775
Eliminar el usuario deseado	Tarea	21.6808964224822	85.4890593332555	2428.18320717026
¿Conoce la clave de acceso?	Compuerta			
Solicitar clave de acceso a tutor	Tarea	59.4337341234104	952.294042426685	11566.5580570775
ExclusiveGateway	Compuerta			
ExclusiveGateway	Compuerta			
Ingresar clave de acceso a credenciales	Tarea	29.9952885817013	919.42241689305	18729.5940861135
NoneEnd	Evento de Fin			
Sincronizar herramienta keepass	Tarea	19.94092311886	918.627079839916	8856.75167130576
Guardar los cambios efectuados en "Credenciales.kdbx"	Tarea	10.7820738252201	82.4748409505792	2414.93607915014
Consulta de usuarios	Proceso	1061.588310838	1171.00680683598	45418.1387980609

Fuente: Elaboración propia, 2022.

5.3.2.4.2 Proceso To-be

Para obtener de los tiempos relacionados con las actividades del proceso 5.2.1.3 Eliminar usuarios, se realizó una entrevista con la organización que se evidencia en el Apéndice O - Minuta EM 08 – 2308. A partir de esa entrevista, para la simulación de este proceso se utilizan dichos tiempos, los cuales se presentan en la Tabla 56. Tiempos To-be Eliminar Usuarios.

Tabla 56. Tiempos To-be Eliminar Usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Informar sobre el requerimiento de borrado del usuario	2	5	3,5	1,5
Analizar requerimiento de borrado del usuario	2	5	3,5	1,5
Brindar respuesta al colaborador	2	5	3,5	1,5
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Solicitar clave de acceso a líder de tribu	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,25
Sincronizar herramienta keepass	0,5	1	0,75	0,25
Eliminar el usuario deseado	2	5	3,5	1,5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,25

Fuente: Elaboración propia, 2022

Tomando como insumo los tiempos expuestos en la Tabla 56. Tiempos To-be Eliminar Usuarios para aplicar la simulación de recursos, se obtiene como resultado de dicha simulación los datos expuestos en la Tabla 57. Simulación recursos Eliminar usuarios To-be.

Tabla 57. Simulación recursos Eliminar usuarios To-be

Recurso	Uso	Costo unitario total	Costo total
Comsultor 1	100.00 %	1553971.3186923	1553971.3186923
Consultor 2	70.78 %	164983.949543067	164983.949543067
Consultor 3	0.80 %	927.285254949173	927.285254949173
Total		1719882.55	1719882.55

Fuente: Elaboración propia, 2022.

Según los datos de la Tabla 57. Simulación recursos Eliminar usuarios To-be, se definieron los siguientes recursos participantes:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

Siendo así, si se toman los recursos detallados anteriormente, las actividades y sus tiempos, que en conjunto forman el proceso 5.2.1.3 Eliminar usuarios, la simulación concluye que el proceso tiene un costo total de ¢1.719.882,55 para un número total de cuarenta ejecuciones. En la Tabla 58. Simulación tiempo Eliminar usuarios To-be, se evidencia el tiempo total y unitario de cada tarea arrojados por la simulación y que conducen al costo mostrado en la Tabla 57. Simulación recursos Eliminar usuarios To-be.

Tabla 58. Simulación tiempo Eliminar usuarios To-be

Nombre	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Crear usuario	25.9413605022866	510.914371135251	12294.1828436647
Inicio			
Ingresar a la herramienta Keepass	6.42827807186245	127.620712824093	1291.49531775101
¿Conoce la clave de acceso?			
Brindar clave de acceso a credenciales	1.24057267785156	72.517200437398	155.248401862096
Solicitar clave a dueño de producto	20.9670846205925	42.2893309054961	105.26681603111
Brindar clave de acceso a credenciales	1.15336366830053	1.59475430732721	4.20632912201938
¿Conoce la clave de acceso?			
Solicitar clave de acceso a tutor	40.7475763917419	135.270715760765	780.668601039404
ExclusiveGateway			
ExclusiveGateway			
Ingresar clave de acceso a credenciales	30.2710206379165	135.552208381092	1410.88915449488
NoneEnd			
Sincronizar herramienta keepass	14.1128532918024	116.938828408042	1165.92914351901
Guardar los cambios efectuados en "Credenciales.kdbx"	3.67166648042132	95.2873863652625	557.108531641252
Informar sobre la creación del usuario	2.64694571893845	103.429695696323	2257.19243267307
Analizar requerimiento de creación de usuario	2.27934720363349	77.4709191887081	1637.86832503219
Brindar respuesta al colaborador	6.9311789664047	77.8851844432071	1950.38120431834
¿Respuesta afirmativa?			
Recepción de respuesta del líder técnico			
NoneEnd			
Recepción de clave de acceso a keepass			
Eliminar el usuario deseado	21.7070628265403	127.171362657122	977.928586180281

Fuente: Elaboración propia, 2022

5.3.2.5 Proceso: Actualización de usuarios

En esta sección se exponen los detalles relacionados con las simulaciones realizadas al proceso *As-Is* y proceso *To-be.*

5.3.2.5.1 Proceso *As-Is*

Tomando como referencia los tiempos obtenidos producto del grupo focal mencionado en el Apéndice N - Minuta EM 07 – 2008, para cada una de las actividades descritas en el proceso 4.4.2.4 Actualización de usuarios, se aplica la distribución normal; se obtuvieron como resultado los promedios y medias por actividad expuestos en la Tabla 44. Tiempos As-Is Crear Usuario.

Tabla 59. Tiempos As-Is Actualización de usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Solicitar clave de acceso a líder de tribu	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,25
Sincronizar herramienta keepass	0,5	1	0,75	0,25
Actualizar el usuario deseado	1	2	1,5	0,5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,25

Fuente: Elaboración propia, 2022.

Al ejecutar la simulación del proceso 4.4.2.4 Actualización de usuarios, tomando como base los tiempos de la Tabla 59. Tiempos As-Is Actualización de usuarios se obtienen los costos detallados en la Tabla 60. Simulación recursos Actualización de Usuarios As Is.

Tabla 60. Simulación recursos Actualización de Usuarios As Is

Recurso	Uso	Costo unitario total	Costo total
Consultor 3	2.14 %	5146.12177402343	5146.12177402343
Consultor 1	98.61 %	3161546.09603033	3161546.09603033
Consultor 2	60.76 %	292217.77869121	292217.77869121
Total		3458910	3458910

Fuente: Elaboración propia, 2022

En relación con la simulación de recursos expuesta en la Tabla 60. Simulación recursos Actualización de Usuarios As Is se definieron los siguientes recursos participantes del proceso:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

Siendo así, si se toman los recursos detallados anteriormente, las actividades y sus tiempos, que en conjunto forman el proceso 4.4.2.4 Actualización de usuarios, la simulación concluye con que el proceso tiene un costo total de ¢3.458.910, para un número total de cuarenta ejecuciones. En la Tabla 61. Simulación tiempo Actualización de usuarios As-Is, se evidencia el tiempo total y unitario de cada tarea arrojados por la simulación y que conllevan al costo mostrado en la Tabla 60. Simulación recursos Actualización de Usuarios As Is.

Tabla 61. Simulación tiempo Actualización de usuarios As-Is

Nombre	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Consulta de usuarios	1026.66845320547	1090.79309569745	42692.1926821594
Inicio			
Ingresar a la herramienta Keepass	0.770524988210964	27.495667529635	574.461404047361
¿Conoce la clave de acceso?			
Brindar clave de acceso a credenciales	1.08196498892607	51.0307285279874	100.899661666038
Solicitar clave a dueño de producto	28.5920431661541	76.2102472411444	723.410917427209
Brindar clave de acceso a credenciales	1.02150959170359	1.99826164632952	23.3437141030775
Actualizar el usuario deseadoo	18.3547611744767	45.0015236879042	1259.43804629575
¿Conoce la clave de acceso?			
Solicitar clave de acceso a tutor	59.4337341234104	952.294042426685	11566.5580570775
ExclusiveGateway			
ExclusiveGateway			
Ingresar clave de acceso a credenciales	19.3733249604838	919.42241689305	18708.3501588711
NoneEnd			
Sincronizar herramienta keepass	16.5655180777425	918.627079839916	8421.86038905802
Guardar los cambios efectuados en "Credenciales.kdbx"	10.7820738252201	43.6634508936788	1313.87033361334

Fuente: Elaboración propia, 2022.

5.3.2.5.2 Proceso To-be

Para simular este proceso se realizó una entrevista con la organización en la cual se obtuvieran los tiempos faltantes de las actividades nuevas agregadas al proceso *To-be* según el diagrama expuesto en la sección 5.2.1.4 Actualizar usuarios. Los tiempos obtenidos de la entrevista demostrada en el Apéndice O - Minuta EM 08 – 2308 se pueden visualizar en la Tabla 62. Tiempos To-be Actualización de usuarios.

Tabla 62. Tiempos To-be Actualización de usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Informar sobre el requerimiento de borrado del usuario	2	5	3,5	1,5
Analizar requerimiento de borrado del usuario	2	5	3,5	1,5
Brindar respuesta al colaborador	2	5	3,5	1,5
Ingresar a herramienta Keepass	0,25	1	0,625	0,375
Solicitar clave de acceso a líder de tribu	20	60	40	20
Solicitar clave a dueño de producto	20	60	40	20
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Brindar clave de acceso a credenciales	1	2	1,5	0,5
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,25
Sincronizar herramienta keepass	0,5	1	0,75	0,25
Actualizar el usuario deseado	1	2	1,5	0,5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,25

Fuente: Elaboración propia, 2022.

Al ejecutar la simulación con los parámetros de tiempos detallados en la Tabla 62. Tiempos To-be Actualización de usuarios, se obtienen los detalles de costos mostrados en la Tabla 63. Simulación recursos Actualización de Usuarios To-be.

Tabla 63. Simulación recursos Actualización de Usuarios To-be

Recurso	Uso	Costo unitario total	Costo total
Consultor 1	100.00 %	1432093.70440855	1432093.70440855
Consultor 2	76.80 %	164983.949543067	164983.949543067
Consultor 3	0.86 %	927.285254949173	927.285254949173
Total		1598004.94	1598004.94

Fuente: Elaboración propia, 2022.

Para la obtención de los resultados de costos del proceso expuestos en la Tabla 63. Simulación recursos Actualización de Usuarios To-be, se utilizaron tres tipos de recursos:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador.
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

Por tanto, tomando la definición de los recursos detallados anteriormente, las actividades y sus tiempos, que en conjunto forman el proceso detallado en la sección 5.2.1.4 Actualizar usuarios, la simulación concluye con que el resultado del proceso tiene un costo total de ¢1.598.004,94 para un número total de cuarenta ejecuciones. En la Tabla 64. Simulación tiempo Actualización de usuarios To-be, se evidencia el tiempo total y unitario de cada tarea arrojado por la simulación y que conducen al costo mostrado en la Tabla 63. Simulación recursos Actualización de Usuarios To-be.

Tabla 64. Simulación tiempo Actualización de usuarios To-be

Nombre	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Crear usuario	25.9413605022866	469.449997938239	11749.3569905694
Inicio			
Ingresar a la herramienta Keepass	6.42827807186245	127.620712824093	1282.98231417027
¿Conoce la clave de acceso?			
Brindar clave de acceso a credenciales	1.24057267785156	72.517200437398	155.248401862096
Solicitar clave a dueño de producto	20.9670846205925	42.2893309054961	105.26681603111
Brindar clave de acceso a credenciales	1.15336366830053	1.59475430732721	4.20632912201938
¿Conoce la clave de acceso?			
Solicitar clave de acceso a tutor	40.4539371702591	135.270715760765	769.251071113207
ExclusiveGateway			
ExclusiveGateway			
Ingresar clave de acceso a credenciales	17.7015410822275	135.552208381092	1342.10865677498
NoneEnd			
Sincronizar herramienta keepass	12.4102525756535	113.70051867136	1035.70479111609
Guardar los cambios efectuados en "Credenciales.kdbx"	3.67166648042132	87.0948076979536	415.31080147693
Informar sobre la creación del usuario	2.64694571893845	103.429695696323	2257.19243267307
Analizar requerimiento de creación de usuario	2.27934720363349	77.4709191887081	1637.86832503219
Brindar respuesta al colaborador	6.9311789664047	77.8851844432071	1950.38120431834
¿Respuesta afirmativa?			
Recepción de respuesta del líder técnico			
NoneEnd			
Recepción de clave de acceso a keepass			
Actualizar el usuario deseado	12.5739962342146	116.829999264724	793.835846879079

Fuente: Elaboración propia, 2022.

5.3.2.6 Proceso: Revisión de usuarios

En este apartado se detallan los resultados obtenidos de aplicar la simulación al proceso *As-Is* y al proceso *To-be.*

5.3.2.6.1 Proceso *As-Is*

Según la brecha identificada y demostrada en la sección 5.1.2 Control y uso de privilegios administrativos, y lo descrito en la entrevista realizada, cuyo detalle puede ser visualizado en la Apéndice O - Minuta EM 08 – 2308, se determina que este proceso no tiene versión *As-Is* debido a que es nuevo, propuesto según el análisis de la brecha entre la situación actual y el marco de referencia seleccionado.

5.3.2.6.2 Proceso *To-be*

Para realizar la respectiva simulación de este proceso *To-be,* se realizó una entrevista con la organización, en la cual se obtuvieron los tiempos de las actividades del proceso según el diagrama expuesto en la sección 5.2.1.6 Revisión de usuarios. Los tiempos obtenidos de la entrevista demostrada en el Apéndice O - Minuta EM 08 – 2308, se pueden visualizar en la Tabla 62. Tiempos To-be Actualización de usuarios.

Tabla 65. Tiempos To-be Revisión de usuarios

Actividad	Duración mínima en minutos	Duración máxima en minutos	Promedio	Desviación
Ingresar a la herramienta Keepass	0,25	1	0,625	0,375
Brindar clave de acceso a credenciales	1	2	1,5	0,70710678
Solicitar clave a dueño de producto	20	60	40	28,2842712
Brindar clave de acceso a credenciales	1	2	1,5	0,70710678
Revisión de los usuarios registrados	20	60	40	28,2842712
Solicitar clave de acceso a Líder de tribu	20	60	40	28,2842712
Ingresar clave de acceso a credenciales	0,5	1	0,75	0,35355339
Sincronizar herramienta keepass	0,5	1	0,75	0,35355339
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1	0,75	0,35355339
Eliminar Usuarios	20	60	40	28,2842712
Actualizar Usuarios	20	60	40	28,2842712

Fuente: Elaboración propia, 2022.

Tomando como insumo los tiempos descritos en la Tabla 65. Tiempos To-be Revisión de usuarios para aplicarlos a las actividades de simulación, se obtienen los costos detallados en la Tabla 66. Simulación recursos Revisión de Usuarios To-be.

Tabla 66. Simulación recursos Revisión de Usuarios To-be

Recurso	Uso	Costo unitario total	Costo total
Consultor 1	100.00 %	8526133.3059099	8526133.3059099
Consultor 2	20.05 %	256456.317894341	256456.317894341
Consultor 3	0.48 %	3050.75217732908	3050.75217732908
Total		8785640.38	8785640.38

Fuente: Elaboración propia, 2022

Según los costos mostrados en la Tabla 66. Simulación recursos Revisión de Usuarios To-be, se definieron tres tipos de recursos:

- Consultor 1: Se refiere a las tareas ejecutadas por el rol de colaborador
- Consultor 2: Se refiere a las tareas ejecutadas por el líder de la tribu.
- Consultor 3: Se refiere a las tareas ejecutadas por el dueño de producto.

En conclusión, si se toma la definición de los recursos detallados anteriormente, las actividades y sus tiempos, que en conjunto forman el proceso detallado en la sección 5.2.1.6 Revisión de usuarios, la simulación concluye con el resultado de que el proceso tiene un costo total de ¢8.785.640,38 para un número total de cuarenta ejecuciones. En la Tabla 67. Simulación tiempo Revisión de Usuarios To-be, se evidencia el tiempo total y unitario de cada tarea arrojado por la simulación y que conducen al costo mostrado en la Tabla 66. Simulación recursos Revisión de Usuarios To-be.

Tabla 67. Simulación tiempo Revisión de Usuarios To-be

Nombre	Tiempo mínimo (m)	Tiempo máximo (m)	Tiempo total (m)
Crear usuario	29.7936315909998	2884.01877276809	53408.7413928837
Inicio			
Ingresar a la herramienta Keepass	6.35414586765003	198.234902188802	2709.38928740546
¿Conoce la clave de acceso?			
Brindar clave de acceso a credenciales	1.23055903112993	71.8467618052483	76.3042835060603
Solicitar clave a dueño de producto	23.8598498660068	104.281707955309	626.520274849949
Brindar clave de acceso a credenciales	1.15336366830053	1.59475430732721	13.8387488198189
¿Conoce la clave de acceso?			
Solicitar clave de acceso a tutor	40.0192337254957	310.890431736017	2288.39828546297
ExclusiveGateway			
ExclusiveGateway			
Ingresar clave de acceso a credenciales	68.3993599812277	346.74076464688	4997.00762431379
NoneEnd			
Sincronizar herramienta keepass	40.2508401851706	440.256224912801	6223.56300156218
Guardar los cambios efectuados en "Credenciales.kdbx"	2.47675779711335	482.649506154087	6252.68345268107
Informar sobre la creación del usuario	2.64694571893845	104.100134328473	2265.23769625887
Analizar requerimiento de creación de usuario	2.27934720363349	76.8004805565583	1632.70357244587
Brindar respuesta al colaborador	6.9311789664047	90.9817331708656	2056.73029648421
¿Respuesta afirmativa?			
Recepción de respuesta del líder técnico			
NoneEnd			
Recepción de clave de acceso a keepass			
Revisión de los usuarios registrados	99.3148009287788	576.361309146305	15692.5465621115

Fuente: Elaboración propia, 2022.

5.3.3 Inventario y control de los activos de software

Según el proceso llevado a cabo para la identificación de la brecha entre la situación actual y el marco de referencia Cobit 5 descrito en la sección 5.1.3 , se identifica que todos los procesos asociados a esta política son nuevos, por tanto, se puede asegurar que no tienen una versión *As-Is* según la situación actual de la empresa.

Basado en el criterio del autor Zlaoui (2022), el cual cita que, si un proceso nuevo forma parte de una propuesta, no es relevante para una investigación realizar simulación sobre el proceso propuesto, pues los tiempos involucrados en dichos procesos no pueden ser calculados sobre la realidad de la empresa pues no han sido implementados.

Por tanto, se puede concluir que al tratarse de una propuesta de procesos y al no contar con su versión *As-Is* no se deben desarrollar simulaciones.

5.4 Medición de la efectividad

En esta sección se muestran los análisis requeridos para demostrar el puntaje que obtendrá cada una de las políticas propuestas para determinar qué tan efectiva es según los rubros especificados en la sección 3.2.3 Axiología.

5.4.1 Defensa contra software malicioso

Para la medición de la efectividad de esta política se toman como base los rubros definidos en la sección 3.2.3 Axiología, los cuales se demuestran bajo las siguientes premisas:

- Para el rubro de documentación existente, se demuestra que la política cuenta con documentación que la respalda, la cual se encuentra contenida en su totalidad en el Apéndice L - y cuyas secciones se encuentran descritas en el apartado Generación de insumo de políticas
- Por tanto, se determina que la política si cuenta con documentación, dando esto un puntaje de 50% sobre este rubro.
- Para el rubro de número de actores, en la Tabla 68. Número de actores defensa contra software malicioso, se citan todos los tipos de actores involucrados en los distintos procesos de la política; da como resultado un total de cinco actores distintos participantes de la política. Dado esto, se determina que la política tiene un porcentaje de 5%.

Tabla 68. Número de actores defensa contra software malicioso

Número de actores					
Proceso	Colaborador	Líder de tribu	Dueño de producto	Tutor	Proveedor
Configuración inicial de antivirus	x	x		x	
Análisis periódicos de los equipos	x	x	x		
Análisis de dispositivos externos	x				
Actualización automática o manual del antivirus	x				
Revisión de archivos descargados o enviados por el cliente	x				
Análisis de validez del antivirus ante nuevas amenazas	x				x

Fuente: Elaboración propia, 2022.

- Para el rubro de aprobaciones necesarias, en la Tabla 69. Aprobaciones necesarias defensa contra software malicioso, se muestra el total de estas, necesarias para cada proceso perteneciente a la política. Estas aprobaciones por proceso fueron obtenidas de los diagramas realizados para los procesos de esta política, los cuales se encuentran en la sección 5.2.2 Defensa contra software malicioso. Siendo así, se determina que como máximo la política requiere de al menos una aprobación, por tanto, el porcentaje obtenido en este rubro es de 25%.

Tabla 69. Aprobaciones necesarias defensa contra software malicioso

Aprobaciones necesarias	
Proceso	Número de aprobaciones
Configuración inicial de antivirus	Sin aprobación necesaria
Análisis periódicos de los equipos	Al menos una
Análisis de dispositivos externos	Sin aprobación necesaria
Actualización automática o manual del antivirus	Sin aprobación necesaria
Revisión de archivos descargados o enviados por el cliente	Sin aprobación necesaria
Análisis de validez del antivirus ante nuevas amenazas	Una como máximo

Fuente: Elaboración propia, 2022.

Por tanto, tomando como base los anteriores puntos, se define en la Tabla 70. Puntaje de efectividad Defensa contra software malicioso, que el puntaje total de efectividad de la política es de 80%, lo cual se traduce en que la política puede ser considerada como efectiva, según lo definido en la sección 3.2.3 Axiología.

Tabla 70. Puntaje de efectividad Defensa contra software malicioso

Rubro	Puntaje obtenido
Documentación existente	50%
Aprobaciones necesarias	25%
Número de actores	5%
Total	80%

Fuente: Elaboración propia, 2022.

5.4.2 Control y uso de privilegios administrativos

Para determinar la efectividad de esta política se deben tomar como guía los rubros definidos en la sección 3.2.3 Axiología, los cuales se demuestran mediante los siguientes puntos:

- Para el rubro de documentación existente, debido a que uno de los entregables de este proyecto corresponde a la documentación relacionada con la propuesta de las políticas de seguridad y que esta se adjunta en su totalidad en el Apéndice L - cuyas secciones se encuentran descritas en el apartado Generación de insumo de políticas, la política sí cuenta con documentación que la respalde. Por tanto, se asigna a este rubro un puntaje de 50%.
- Para el rubro de número de actores, en la Tabla 71. Número de actores Control y uso de privilegios administrativos, se muestra el total de actores participantes de los distintos procesos pertenecientes a la política y en esta se evidencia que en la política participa un total de cuatro actores distintos. Por tanto, se determina que este rubro tiene un puntaje de 5%.

Tabla 71. Número de actores Control y uso de privilegios administrativos

Número de actores				
Proceso	Colaborador	Líder de tribu	Dueño de producto	Mentor
Configuración inicial	x	x		x
Consulta de usuarios	x	x	x	
Eliminar usuarios	x	x	x	
Actualizar usuarios	x	x	x	
Crear usuario	x	x	x	
Revisión de usuarios	x	x	x	

Fuente: Elaboración propia, 2022.

- Para el rubro de aprobaciones necesarias, en la Tabla 72. Aprobaciones necesarias Control y uso de privilegios administrativos, se muestran las necesarias para cada proceso que pertenece a la política. Esta tabla evidencia que el número máximo de aprobaciones para un proceso es de uno, por tanto, se determina que para este rubro el puntaje es de 25%. Las aprobaciones se obtienen según los diagramas detallados en la sección 5.2.1 Control y uso de privilegios administrativos.

Tabla 72. Aprobaciones necesarias Control y uso de privilegios administrativos

Aprobaciones necesarias	
Proceso	Número de aprobaciones
Configuración inicial	Sin aprobación necesaria
Consulta de usuarios	Sin aprobación necesaria
Eliminar usuarios	Máximo una aprobación
Actualizar usuarios	Máximo una aprobación
Crear usuario	Máximo una aprobación
Revisión de usuarios	Sin aprobación necesaria

Fuente: Elaboración propia, 2022.

En conclusión, de los anteriores puntos detallados, cuyos puntajes se encuentran en modo resumen en la Tabla 73. Puntaje de efectividad Control y uso de privilegios administrativos, se determina que el porcentaje total de la política es de 80%, lo cual la convierte en una política efectiva, según lo definido en la sección 3.2.3 Axiología.

Tabla 73. Puntaje de efectividad Control y uso de privilegios administrativos

Rubro	Puntaje obtenido
Documentación existente	50%
Aprobaciones necesarias	25%
Número de actores	5%
Total	80%

Fuente: Elaboración propia, 2022.

5.4.3 Inventario y control de los activos de software

Con el objetivo de determinar la efectividad de esta política, se deben evaluar los rubros definidos en la sección 3.2.3 Axiología, los cuales se demuestran mediante los siguientes puntos:

- Para el rubro de *documentación existente,* debido a que este proyecto entrega a la organización documentación relacionada con la propuesta de las políticas de seguridad y que esta se adjunta en su totalidad en el Apéndice L - cuyas secciones se encuentran descritas en el apartado Generación de insumo de políticas la política, se determina que la política sí cuenta con documentación que la respalde. Por tanto, se asigna a este rubro un puntaje de 50%.
- Para el rubro de *número de actores,* en la Tabla 74. Número de actores Inventario y control de activos de software, se demuestra que en los procesos asociados a esta política solo participa un tipo de actor, por tanto, se asigna a este rubro un puntaje de 25%.

Tabla 74. Número de actores Inventario y control de activos de software

Número de actores			
Proceso	Colaborador	Líder de tribu	Dueño de producto
Registro de activos de software	x		
Control de activos de software	x		
Eliminar un activo de software	x		
Revisión de numeración de activos de software	x		

Fuente: Elaboración propia, 2022.

- Para el rubro de aprobaciones necesarias, en la Tabla 75. Aprobaciones necesarias Inventario y control de activos de software, se detalla que los procesos pertenecientes a la política no requieren de aprobaciones; esto, según el análisis efectuado sobre los diagramas incluidos en la sección 5.2.3 Inventario y control de los activos de software. Por tanto, el porcentaje asignado a este rubro para esta política es de 25%

Tabla 75. Aprobaciones necesarias Inventario y control de activos de software

Aprobaciones necesarias	
Proceso	Número de aprobaciones
Registro de activos de software	Sin aprobación necesaria
Control de activos de software	Sin aprobación necesaria
Eliminar un activo de software	Sin aprobación necesaria
Revisión de numeración de activos de software	Sin aprobación necesaria

Fuente: Elaboración propia, 2022.

Para concluir con la medición de la efectividad de esta política, si se toman los anteriores puntos detallados, los cuales se encuentran en modo resumen en la Tabla 76. Puntaje de efectividad Inventario y control de activos de software, se determina que el porcentaje total de la política es de 100% lo cual la convierte en una política efectiva, según lo definido en la sección 3.2.3 Axiología.

Tabla 76. Puntaje de efectividad Inventario y control de activos de software

Rubro	Puntaje obtenido
Documentación existente	50%
Aprobaciones necesarias	25%
Número de actores	25%
Total	100%

Fuente: Elaboración propia, 2022.

5.5 Análisis financiero

En esta sección se pretende dar detalle de los cálculos necesarios para asegurar la viabilidad financiera de la implementación de las políticas propuestas y de sus determinados procesos, así como un análisis del costo total que tuvo la organización producto del desarrollo de esta propuesta de políticas de seguridad.

5.5.1 Análisis financiero de las políticas

Para determinar la viabilidad financiera de las políticas de seguridad propuestas se utilizará la métrica denominada Retorno de la inversión (ROI, por sus siglas en inglés). Según Cueva (2001) esta métrica es usada para determinar la ganancia de una empresa sobre una determinada inversión realizada, por tanto, con ella se puede determinar si una inversión vale la pena o no. Para el cálculo del retorno de inversión se utiliza la fórmula mostrada en la Ilustración 45. Fórmula ROI.

Ilustración 45. Fórmula ROI

$$\frac{\text{Ganancia} - \text{Inversión}}{\text{Inversión}}$$

Fuente: Elaboración propia, 2022.

Para determinar el retorno de inversión de algunas de las políticas, es necesario conocer el monto total en inventario de las computadoras laptops que utilizan los colaboradores para sus labores diarias. Para obtener este dato, se realizó una sesión con la organización la cual se documentó en el Apéndice P - Minuta EM 09 – 2508, donde se indica que el total corresponde a ₡20.000.000; esto significa una valoración de ₡500.000 por equipo.

Además, con el fin de calcular el monto relacionado con el colaborador que realiza la investigación, se utilizará como base el salario mínimo establecido por el Ministerio de Trabajo de Costa Rica, el cual, según MTSS (2022) es de ¢705.514,95 mensuales para el segundo semestre del 2022. A este monto, se le debe agregar el monto de cargas sociales, el cual corresponde a 26.5% sobre el total. Para determinar el monto final de salario, se debe realizar el siguiente cálculo:

¢705.514,95 * 1.265 = ¢892.476,42

En la Tabla 77. Salario investigador, se muestra el detalle de los montos utilizados como salario base.

Tabla 77. Salario investigador

Salario mínimo licenciatura universitaria	
Mensual	¢892.476,42
Semanal	¢223.119,105
Diario	¢44.623,82
Hora	¢5577,98

Fuente: Elaboración propia, 2022.

5.5.1.1 Control y uso de privilegios administrativos

Para el análisis financiero de esta política es necesario tomar en cuenta los análisis de recursos realizados sobre los procesos *As-Is* y los procesos *To-be*. Según los análisis de recursos detallados en la sección 0 Según la identificación de la brecha entre la situación actual y el marco de referencia Cobit 5 descrita en la sección 5.1.1 Defensa contra software malicioso, se identifica que todos los procesos asociados a esta política son nuevos, por tanto, se puede asegurar que estos procesos no tienen una versión *As-Is* según la situación actual de la empresa.

El autor Zlaoui (2022) menciona que, los estudios de simulación son de interés cuando hay una falta de orientación en la literatura o cuando los métodos son novedosos. Según esto, los procesos asociados a esta política no son sujetos a estudios de simulación dado que cuentan con la guía del marco de referencia, además, no se pueden considerar como novedosos ya que, aunque sean nuevos en la empresa, si son implementados por muchas organizaciones en la actualidad. Esta premisa se determinó según la revisión documental detallada en Apéndice Q - Minuta RV 04 – 2208.

Por tanto, se puede definir que, si un proceso nuevo forma parte de una propuesta, no toma relevancia realizar simulación sobre el proceso propuesto, ya que los tiempos involucrados

en dichos procesos no pueden ser calculados sobre la realidad de la empresa pues no han sido implementados

Control y uso de privilegios administrativos, en la Tabla 78. Costo total política Control y uso de privilegios administrativos As-Is, se puede observar el total de los costos de la sumatoria de los procesos *As-Is.* Entretanto, en la Tabla 79. Costo total política Control y uso de privilegios administrativos To-be, se evidencia el total de la sumatoria de los costos de los procesos *To-be.*

Tabla 78. Costo total política Control y uso de privilegios administrativos As-Is

Proceso	Costo
Configuración Inicial	6.933.358,69
Crear Usuario	5.713.715,19
Consulta de usuarios	2.666.868,40
Eliminar usuarios	3.635.741,12
Actualización de usuarios	3.458.910,00
Total	22.408.593,40

Fuente: Elaboración propia, 2022.

Tabla 79. Costo total política Control y uso de privilegios administrativos To-be

Proceso	Costo
Configuración Inicial	6.933.358,69
Crear Usuario	1.378.079,66
Consulta de usuarios	2.666.868,40
Eliminar usuarios	1.719.882,55
Actualización de usuarios	1.598.004,94
Revisión de usuarios	8.785.640,38
Total	23.081.834,62

Fuente: Elaboración propia, 2022.

Siendo así, al aplicar la métrica *ROI* se definen las siguientes premisas:

- Para el cálculo de la ganancia se debe determinar la diferencia entre el costo total del escenario *As-Is,* detallado en la Tabla 78. Costo total política Control y uso de privilegios administrativos As-Is, y el costo total del escenario *To-be* expuesto en la Tabla 79. Costo total política Control y uso de privilegios administrativos To-be. Al realizar el cálculo mencionado, se obtiene el siguiente resultado:

  ₡22.408.593,40 - ₡23.081.834,62 = -₡673.241,22

  En conclusión, el resultado total de la ganancia es de -₡673.241,22.
- Para la inversión, es necesario contabilizar las dieciséis semanas en las que el investigador desarrolló la propuesta de políticas y sus determinados procesos. En la Tabla 77. Salario investigador se muestra el costo relacionado con el investigador en distintas medidas de tiempo. Para el intervalo semanal, el costo asociado es de ¢223.119,105, además, la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado con lo anteriormente mencionado sería el siguiente:

  ¢223.119,105 * 16 = ¢3.569.905,68

  Por tanto, el costo total de la inversión es de ¢3.569.905,68

Siendo así, y para brindar el resultado asociado a la métrica *ROI* descrita en la Ilustración 45. Fórmula ROI, y tomando en cuenta la ganancia e inversión descritas anteriormente, el cálculo

se realiza según lo mostrado en la Ilustración 46. Cálculo ROI Control y uso de privilegios administrativos.

Ilustración 46. Cálculo ROI Control y uso de privilegios administrativos

$$\frac{-₡673.241,22 - ¢3.569.905,68}{¢3.569.905,68} = -1.18$$

Fuente: Elaboración propia, 2022

Según lo mostrado en la Ilustración 46. Cálculo ROI Control y uso de privilegios administrativos, se determina que el retorno de la inversión es el resultante del cálculo:

-1.18 * 100 = -118%

Como se evidencia, el retorno de la inversión es negativo, lo cual significa que para esta política la inversión está generando pérdida. Sin embargo, es importante aclarar que este era un resultado esperado, ya que la versión *To-be* de la política incluye actividades y procesos extra con el fin de cumplir con el marco de referencia, según se evidencia en la sección 5.1.2 Control y uso de privilegios administrativos. Es importante destacar que, dada la naturaleza del proyecto, el retorno de la inversión no es una métrica decisiva para medir el éxito del proyecto, pues el propósito de dicha investigación es estandarizar la política y adecuarla a la buena práctica seleccionada.

5.5.1.2 Defensa contra software malicioso

Para la realización del análisis financiero asociado con esta política, es necesario reconocer que, según lo definido en el apartado 5.1.1 Defensa contra software malicioso, esta política forma parte de la propuesta realizada pero no cuenta con desarrollo de procesos *As-Is* debido a que no pertenece al quehacer cotidiano de la empresa. Además, en la sección 5.3.1 Defensa contra software malicioso, se determinan las razones por las cuales no se realizó simulación para los escenarios *As-Is* y *To-be.*

Por tanto, para el cálculo de la métrica *ROI,* se debe tomar en cuenta la siguiente información:

- En cuanto a la ganancia, se realizó una revisión documental detallada en el Apéndice R – Minuta RV 05 – 2308 y se determinó que una de las principales dificultades de no contar con herramientas antivirus es el riesgo relacionado al robo o desaparición de información, sobre esto, Statista (2017) menciona que para el año 2020 un 35% de la información almacenada en los repositorios organizacionales requiere de medidas de seguridad, pero se encuentra desprotegida. Siendo así, en el Apéndice P - Minuta EM 09 – 2508 se determina que el costo total de las laptops, que son los principales repositorios de información de la organización, es de ₡20.000.000, por tanto, el cálculo a realizar sería el siguiente:

  ₡20.000.000 * 0.35 = ₡7.000.000

  Por tanto, según las estadísticas aportadas, los mencionados ₡7.000.000 corresponden a la ganancia obtenida de implementar esta política.
- Respecto al costo total de la inversión para esta política, es necesario tomar en cuenta las dieciséis semanas en las que el investigador desarrolló la propuesta. Según se muestra en la Tabla 77. Salario investigador, el costo relacionado con el investigador, de forma semanal, es de ¢223.119,105 y la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado con lo anteriormente mencionado sería el siguiente:

  ¢223.119,105 * 16 = ¢3.569.905,68

  Por tanto, el costo total de la inversión es de ¢3.569.905,68.

En conclusión, y tomando en cuenta las premisas detalladas sobre ganancia e inversión, y basándose en la Ilustración 45. Fórmula ROI, el cálculo de la métrica *ROI* se realiza según lo indicado en la Ilustración 47. Cálculo ROI Defensa contra software malicioso.

Ilustración 47. Cálculo ROI Defensa contra software malicioso

$$\frac{₡7.000.000 - ¢3.569.905,68}{¢3.569.905,68} = 0,96$$

Fuente: Elaboración propia, 2022.

Según lo mostrado en la Ilustración 47. Cálculo ROI Defensa contra software malicioso, se determina que el retorno de la inversión es el resultante del cálculo:

0,96 * 100 = 96%

Esto se puede traducir a un retorno de la inversión alto. Sin embargo, se debe recordar que el desarrollo de esta propuesta está enfocado en el uso y estandarización de las políticas de seguridad en la organización, por lo que, de momento, no está en el alcance del proyecto proyectar retornos de inversión altos provenientes de la aplicación de las políticas. Por tanto, se concluye que el *ROI* no es una métrica determinante para el éxito de la propuesta.

5.5.1.3 Inventario y control de los activos de software

Para la realización del análisis financiero de esta política, se debe tomar en cuenta que, según lo definido en la sección 5.1.3 Inventario y control de los activos de software., esta política es nueva en la organización, sección en la que también se demostraron las razones por las cuales no se contempló el escenario *As-Is.* Sumado a esto, en el apartado 5.3.3 Inventario y control de los activos de software, se determinan las razones por las cuales no se realizó simulación para ninguno de los escenarios.

Por tanto, para el cálculo de la métrica *ROI,* se deben tomar en cuenta las premisas detalladas a continuación:

- Para determinar la ganancia, es necesario conocer que una de las principales desventajas de no ejecutar procesos relacionados con el inventariado de los activos de software es la

pérdida que se pueda dar de estos. Para esto, Seareach (2018) menciona que las computadoras tipo laptops son uno de los activos más propensos a extraviarse, con un porcentaje de 14% de probabilidad de extravío sobre el total de equipos laptops. Siendo así, en el Apéndice P - Minuta EM 09 – 2508 se determinó que la organización cuenta con un total de cuarenta laptops, por tanto, el 14% de ese total corresponde a 5.6, lo que para efectos prácticos se tomará como un total de cinco laptos. En el Apéndice P - Minuta EM 09 – 2508 se menciona que cada equipo está valorado en ₡500.000, por tanto, el monto total de laptops propensas a extraviarse se calcula de la siguiente manera:

₡500.000 * 5 = ₡2.500.000

Además, Seareach (2018) comenta que cuando un activo se extravía es común pensar que basta únicamente con reponerlo, sin embargo, la pérdida de una laptop conduce a actividades y pérdida de información que tienen un costo adicional asociado. Este costo es determinado en un total de £249 (doscientos cuarenta y nueve libras esterlinas) por equipo, lo cual se traduce a ₡186.592,00. Para el total de laptops propensas a extraviarse el cálculo sería de la siguiente manera:

₡186.592,00 * 5 = ₡932.960

Dados los anteriores cálculos, en la Tabla 80. Ganancia total Inventario y control de activos de software, se muestra el resumen y suma total de la ganancia esperada; se tiene como total la suma de ₡3.435.960. Estas estadísticas son tomadas como ganancia, ya que es el ahorro que tendría la organización si implementa la política y procesos propuestos.

Tabla 80. Ganancia total Inventario y control de activos de software

Estadística	Costo
Costo total de laptops propensas a extraviarse	₡2.500.000
Costos asociados al extravío de las laptops	₡932.960
Total	₡3.435.960

Fuente: Elaboración propia, 2022.

- Respecto a la inversión para esta política, es necesario tomar en cuenta las dieciséis semanas con las que contó el investigador para el desarrollo de la propuesta. Según se

muestra en la Tabla 77. Salario investigador el costo relacionado al investigador de forma semanal es de ¢223.119,105 y la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado a lo anteriormente mencionado sería el siguiente:

¢223.119,105 * 16 = ¢3.569.905,68

Por tanto, el costo total de la inversión es de ¢3.569.905,68.

Tomando en cuenta las anteriores premisas y basado en la Ilustración 45. Fórmula ROI, el cálculo para determinar la métrica *ROI* sería el que se evidencia en la Ilustración 48. Cálculo ROI Inventario y control de los activos de software.

Ilustración 48. Cálculo ROI Inventario y control de los activos de software

$$\frac{¢3.435.960 - ¢3.569.905,68}{¢3.569.905,68} = -0,03$$

Fuente: Elaboración propia, 2022.

Según lo mostrado en la Ilustración 48. Cálculo ROI Inventario y control de los activos de software, se determina que el retorno de la inversión es el resultante del cálculo:

-0,3 * 100 = -30%

Lo que se puede traducir a un retorno de la inversión negativo que implica una inversión mayor a lo percibido como ganancia. Sin embargo, cabe destacar que esta métrica arroja el retorno de la inversión sobre la situación actual, lo que quiere decir que si la organización sigue en crecimiento el retorno de la inversión crecerá. Además, se debe recordar que el desarrollo de esta propuesta está enfocado en la orientación de las políticas de seguridad hacia las buenas prácticas, y en estandarizas su uso sobre la totalidad de tribus de la organización, por tanto, el retorno de la inversión no es un indicador clave para el éxito de esta propuesta.

5.5.2 Costo de desarrollo de la propuesta

En esta sección, se pretende brindar detalle aproximado sobre monto ahorrado por la organización relacionado al desarrollo de la propuesta.

Como punto principal, es necesario aclarar que esta propuesta fue realizada ad honoren, con el objetivo de atacar la problemática planteada en la investigación. Para el cálculo del costo, en la Tabla 77. Salario investigador se determina que el costo semanal equivale a ¢223.119,105, mientras que la duración comprende un total de dieciséis semanas, siendo así, el cálculo sería el siguiente:

¢223.119,105 * 16 = ¢3.569.905,68

Ante esto, el anterior cálculo muestra el costo de desarrollar esta propuesta, permitiendo visualizar un ahorro de ¢3.569.905,68 para la organización.

5.6 Generación de insumo de políticas

Como parte de los entregables definidos en la sección 1.7 Entregables, en el Apéndice M - Propuesta de políticas de seguridad – Xumtech, se adjunta el documento elaborado con los resultados obtenidos del proyecto. Este documento será entregado a la organización como prueba de la investigación realizada y la empresa podrá hacer uso de él a conveniencia.

6 Conclusiones

Esta sección muestra las conclusiones obtenidas de la investigación realizada. Estas conclusiones estarán separadas de acuerdo con los objetivos específicos de la organización descritos en el apartado 1.4.2 Objetivos Específicos así como las conclusiones sobre el objetivo general demostrado en la sección **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.

Objetivo 1: Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.

- Según el análisis de los instrumentos para recopilar información, se identifica que las políticas de seguridad son aplicadas de forma aislada por parte de las tribus, lo cual provoca la gestión desarticulada de los procesos asociados a las políticas.
- Actualmente, no existe en la organización una política establecida para el uso de herramientas *antimalware* que brinde a los colaboradores una guía sobre el uso de este tipo de herramientas.
- La organización no cuenta con procesos relacionados con el registro y control de los activos de software con los cuales se cuenta, así como de los responsables de su cuidado y mantenimiento.
- Se evidencia que existen procesos organizacionales para el registro y uso de accesos a herramientas empresariales y plataformas informáticas de clientes.
- Con un puntaje de 90%, se identifica que la política denominada “Defensa contra software malicioso” tiene oportunidad de mejora enfocada en su documentación, estandarización en la organización y número de escalamientos.
- Se determina que la política “Control y uso de privilegios administrativos”, con un puntaje de 20%, tiene una oportunidad de mejora baja enfocada en la poca estandarización de sus procesos en la organización.
- El cálculo de la oportunidad de mejora para la política de “Inventario y control de los activos de software” arroja un 90% de puntaje e indica que los procesos de esta política deben mejorar en cuento a estandarización, escalamiento y documentación existente.

Objetivo 2: Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria.

- Se identifica la necesidad de realizar la propuesta del proceso denominado "Configuración inicial" para la política "Defensa contra software malicioso", esto para brindar guía a los colaboradores sobre la instalación de herramientas para prevenir los ataques de software malicioso.
- Inexistencia de un proceso que permita validar la efectividad de las herramientas contra software malicioso ante nuevas amenazas y que forme parte de la política de "Defensa contra software malicioso".
- La no existencia de procesos enfocados en la revisión de los insumos enviados a la organización por correo electrónico o descargados de la web pone en riesgo los activos tangibles e intangibles de la empresa; se concluye que esta práctica debería formar parte de la política de "Defensa contra software malicioso".
- La falta de madurez en la infraestructura tecnológica de la organización no permite la propuesta de medidas de protección de alta gama.
- Al tratarse de una organización pequeña, no se cuenta con áreas específicas dedicadas a la protección de datos, tampoco con una definición de roles dedicados específicamente a laborar en temas de seguridad informática.
- Para la política de "Control y uso de privilegios administrativos", se identifica la necesidad de que cualquier modificación por realizar sobre algún acceso cuente con un debido análisis y aprobación de la solicitud.
- Inexistencia de procesos relacionados con la revisión y depuración de usuarios existentes en la herramienta Keepass.
- No existen procesos relacionados con la inspección de los activos de software existentes contra el inventario creado.

Objetivo 3: Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis financiero para la validación de la efectividad de las mejoras propuestas.

- Se concluyó que la política "Defensa contra software malicioso" no puede ser simulada debido a que se trata de un conjunto de procesos que forman parte de una propuesta, por lo que no se puede hacer una medición real de los tiempos involucrados en las actividades de dichos procesos.
- Respecto a la política denominada "Inventario y control de los activos de software", se determina que no se puede aplicar simulación sobre sus procesos ya que, al formar parte de la propuesta como nuevos procesos, no se puede realizar una medición de los tiempos involucrados en cada una de las actividades.
- Para la política de "Control y uso de privilegios administrativos" se determinó mediante la simulación de costos de los recursos involucrados que el escenario *As-Is* tiene un costo de ₡ 22.408.593,40, mientras que el escenario *To-be* tiene un costo de ₡ 23.081.834,62para un total de cuarenta ejecuciones diarias.
- Se determina que las políticas propuestas presentan una alta efectividad según la identificación de la brecha y medición de la efectividad llevadas a cabo.
- El análisis financiero realizado para la política "Control y uso de privilegios administrativos" y bajo la métrica de retorno de la inversión arroja un resultado de -118%, lo cual implica que la política está generando perdidas producto de las nuevas actividades y procesos propuestos producto del análisis de la brecha.
- Se determina que la política "Defensa contra software malicioso" arroja un retorno de inversión de 96%, esto determinado sobre la ganancia esperada de la protección de equipos e información.
- La política de "Inventario y control de activos de software" presenta un retorno de inversión de -30%, basado en las ganancias obtenidas de la correcta gestión de los activos.
- Se determina el costo de realización de la propuesta de políticas de seguridad en ¢3.569.905,68; esta investigación se realizó de forma *ad honorem.*

Objetivo general: Elaborar una propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech en un lapso de dieciséis semanas para la estandarización de los procesos asociados a las políticas de seguridad utilizadas en la organización.

- Se determina que las políticas propuestas a la organización son efectivas basado en los rubros definidos bajo el enfoque alternativo de la metodología.
- La propuesta de políticas de seguridad entregada a la organización fue realizada basada en buenas prácticas de la industria como Cobit 5 y Controles CIS.
- La propuesta de políticas de seguridad promueve la estandarización en la organización ya que su desarrollo tomó en cuenta criterios y realidades de las tribus existentes actualmente.

7 Recomendaciones

En esta sección se detallan los puntos recomendados por el investigador para cada uno de los objetivos definidos.

Objetivo 1: Analizar los procesos y políticas de seguridad de la información actuales para la identificación de oportunidades de mejora mediante análisis documental y entrevistas.

- Proyectar esfuerzos en que las tribus y sus integrantes comprendan la necesidad de implementar políticas de seguridad de la información y de los activos.
- Tomar los criterios definidos para identificar una oportunidad de mejora para cada política de seguridad y sus procesos asociados que se quieran implementar en la organización.

Objetivo 2: Proponer, según el caso, la definición o actualización de políticas de seguridad para el desarrollo del conjunto de procesos asociados a cada política según la brecha identificada entre la situación actual y las mejores prácticas de la industria

- Establecer en la organización roles funcionales encargados de actividades relacionadas con la gestión, vigilancia y aplicación de las políticas de seguridad; esto para validar el cumplimiento y estandarización de las políticas.
- Aunque en la organización existan políticas de libre acceso a la información, es recomendable definir el tipo de información de alto riesgo y establecer roles que puedan accederla o no hacerlo.
- Establecer sobre cada activo de la organización los objetivos que cada uno de estos debe cumplir; la finalidad es evaluar cuando un activo deja de dar valor a la organización y pueda ser relevado.

Objetivo 3: Evaluar las políticas y procesos de seguridad propuestos con respecto a la situación actual mediante el desarrollo de simulaciones y de un análisis costo beneficio para la validación de la efectividad de las mejoras propuestas.

- Se considera relevante implementar un plan de comunicación dirigido a los colaboradores de la organización para concienciar sobre el uso y correcta aplicación de los procesos relacionados con la protección contra software malicioso, pues de esto dependerá el nivel de protección de la información que la organización alcance.
- Aunque los retornos de inversión resultantes del análisis financiero, aplicados a las políticas propuestas son bajos, se recomiendan los modelos *To-be* propuestos, pues el objetivo principal del proyecto es generar estandarización de las políticas de seguridad en las tribus y no generar, en primera instancia, ganancia económica.
- Formalizar la documentación aportada por esta investigación como oficial de la organización, para que la propuesta pueda ser aplicada por los colaboradores de las distintas tribus.
- Publicar la documentación brindada como entregable en la herramienta *Confluence*, de modo que todos los colaboradores tengan acceso, pues esta funciona como el repositorio organizacional de información.

8 Referencias

Abarca, F. (s.f). Teorema del límite central: Desigualdades de Chebyshev y Markov y ley de los grandes números. https://www.kerwa.ucr.ac.cr/bitstream/handle/10669/83895/12%20Teorema%20del%20li%CC%81mite%20central%20y%20otros.pdf?sequence=13&isAllowed=y

Becerra, O. (2012). Elaboración de Instrumentos de Investigación. https://www.academia.edu/12594995/Elaboraci%C3%B3n_de_Instrumentos_de_Investigaci%C3%B3n

Bizagi. (s.f). Bizagi Modeler. https://www.bizagi.com/es/plataforma/modeler#:~:text=Software%20gratuito%20de%20mapeo%20y%20modelamiento%20de%20procesos%20de%20negocio%20%2D%20Bizagi%20Modeler

CAIGG. (2016). Conceptos Generales sobre enfoque de procesos de negocio. http://54.148.75.48/bitstream/handle/123456789/115/DOCUMENTO-TECNICO-88-CONCEPTOS-GENERALES-SOBRE-ENFOQUE-DE-PROCESOS-DE-NEGOCIOS.pdf?sequence=1&isAllowed=y

Central Oregon Community College (s.f). CIA Triad: Confidentiality, Integrity and Availability. https://www.cocc.edu/departments/cio/infosec/concepts/cia-triad.aspx

Confluence (s.f). Confluence. https://www.atlassian.com/es/software/confluence/features?tab=enterprise-plan

Cuevas, C. (2001). Medición del desempeño: Retorno sobre inversión, ROI; Ingreso residual, IR; Valor económico Agregado, EVA; Análisis Comparado. https://www.redalyc.org/pdf/212/21207901.pdf

Duque Méndez, N. (2002). Diseño e implementación de una política de seguridad. Universidad Nacional de Colombia - Sede Manizales. https://repositorio.unal.edu.co/bitstream/handle/unal/60125/dise%c3%b1oeimplementaciondeunapoliticadeseguridad.pdf?sequence=1&isAllowed=y

Encalada, C., Cordero, D. (2016). Guía de auditoría para la evaluación del control interno de seguridad de la información con enfoque Cobit 5: Caso Universidad Católica de Cuenca (UCACUE). https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/204/pdf

García, T. (2003). El cuestionario como instrumento de investigación/evaluación. http://www.univsantana.com/sociologia/El_Cuestionario.pdf

Gartner. (2020). Control Objectives for Information and Related Tecnhnology (COBIT). https://www.gartner.com/en/information-technology/glossary/cobit-control-objectives-for-information-and-related-technology

Gutiérrez, H (2010). Calidad total y productividad. http://students.aiu.edu/submissions/profiles/resources/onlineBook/n8A2y8_Calidad%20Total%20y%20Productividad-(2010).pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación: Roberto Hernández Sampieri, Carlos Fernández Collado y Pilar Baptista Lucio (6a. ed. --.). McGraw-Hill.

ISACA. (2012). COBIT 5. United States: ISACA

Jiménez, J (2020). Propuesta de solución para el proceso de aseguramiento de la calidad de software en la empresa SUUM technologies apoyado en estándares y buenas prácticas de la industria. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/13207/TFG_Juliano_Jimenez_Castillo.pdf?sequence=1&isAllowed=y

Keepass. (s.f). Keepass features. https://keepass.info/features.html

Mallar, M. (2010). La gestión por procesos: Un enfoque de gestión eficiente. https://www.redalyc.org/pdf/3579/357935475004.pdf

MTSS. (2022). Lista de salarios mínimos por ocupación, segundo semestre 2022. https://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salario

Reidl, L. (2012). Marco Conceptual en el proceso de investigación. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-50572012000300007

PDF CIS CONTROLS

Seareach. (2018). Lost or Stolen Assets Cost Businesses Mora than Just Replacement Items. https://www.seareach.co.uk/blog/lost-or-stolen-assets-cost-more/

Sierra, M. (2014). Propuesta de mejora para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, basado en el estándar ISO/IEC 27002:2005. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11032/propuesta_mejora_politicas_seguridad_informacion.pdf?sequence=1&isAllowed=y

Statista. (2017). Actual status of data security worldwide from 2010 to 2025. https://www.statista.com/statistics/815167/worldwide-actual-status-of-data-security/

Suum Technologies. (2020). SUUM Technologies – Tecnología a su alcance. https://suumtech.com/

Zlaoui, K. (2022). Using Simulation Studies to Motivate Modelling Decisions. https://towardsdatascience.com/using-simulation-studies-to-motivate-modelling-decisions-be8bae2cd1c2

9 Apéndices

Apéndice A - Temas entrevista cerrada

Defensa Anti-Malware

1. ¿Cuenta su equipo con antivirus (antimalware)?
2. ¿Conoce usted si Xumtech cuanta con políticas de uso de antivirus?
3. ¿De contar con antivirus: ¿Qué gestiones realiza o realizaría con este?
4. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
5. ¿Su tribu aplica políticas de gestión de antivirus?

Uso de keepass

1. ¿Ha usado usted la herramienta keepass?
2. ¿Sabe de la existencia de documentación relacionada al correcto uso de keepass?
3. ¿Utiliza su tribu reglas sobre el uso de keepass?
4. ¿Qué gestiones realiza con el keepass?
5. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?

Inventario de software

1. ¿Conoce sobre la existencia de documentación relacionada a software con los que cuenta Xumtech?
2. ¿Utiliza su tribu algún inventario sobre software existente?
3. De necesitar alguna aprobación/información relacionada a este tema, ¿Con cuáles personas lo consultaría?

Apéndice B - Encuesta a líderes técnicos y consultores

Políticas de seguridad y procesos asociados

Este formulario tiene como finalidad obtener la información necesaria sobre la situación actual de la empresa Xumtech en cuanto a políticas de seguridad y procesos asociados a estas. Toda la información aqui brindada será privada y será de uso exclusivo para el trabajo final de graduación de Sergio Arroyo.

*Obligatorio

1. Nombre *

2. Tribu *

Marca solo un óvalo.

- ◯ Tribu Alex
- ◯ Tribu Jose
- ◯ Tribu Andre
- ◯ Tribu Maya
- ◯ Tribu Dunamis
- ◯ Tribu Bulwak
- ◯ Tribu Onix

3. Puesto *

Marca solo un óvalo.

- ◯ Consultor(a)
- ◯ Líder técnico

Antivirus

4. ¿Cuenta su equipo con antivirus (antimalware)? *

   Marca solo un óvalo.

   - ◯ Si
   - ◯ No

5. ¿Conoce usted si Xumtech cuenta con políticas de uso de antivirus? *

   Marca solo un óvalo.

   - ◯ Si
   - ◯ No

6. ¿Qué gestiones realiza o realizaría con un antivirus? (Marque y/o agregue las opciones que considere correctas) *

   Selecciona todos los que correspondan.

   - ☐ Análisis periódicos del equipo
   - ☐ Análisis de memorias externas (discos duros, memorias USB, etc)
   - ☐ Actualización automática o manual del antivirus
   - Otro: ☐ _____

7. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría? *

   Marca solo un óvalo.

   - ◯ Con el líder de tribu
   - ◯ Con el líder de tribu y Alex Ureña
   - ◯ Solo con Alex Ureña
   - ◯ Con el líder de tribu, algún otro compañero y Alex Ureña

8. ¿Aplica su tribu políticas de gestión de antivirus? *

Marca solo un óvalo.

- Sí
- No

Keepass

9. ¿Ha usado usted la herramienta keepass? *

Marca solo un óvalo.

- Sí
- No

10. ¿Sabe de la existencia de documentación relacionada al correcto uso de keepass? *

Marca solo un óvalo.

- Si
- No

11. ¿Utiliza su tribu reglas sobre el uso de keepass? *

Marca solo un óvalo.

- Sí
- No

12. ¿Qué gestiones realiza con el keepass? (Marque y/o agregue las opciones que considere correctas) *

Selecciona todos los que correspondan.

- [ ] Consulta de usuarios
- [ ] Agregar usuarios
- [ ] Eliminar usuarios
- [ ] Sincronización de usuarios
- [ ] Otro: _____

13. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría? *

Marca solo un óvalo.

- ◯ Con el líder de tribu
- ◯ Con el líder de tribu y Alex Ureña
- ◯ Solo con Alex Ureña
- ◯ Con el líder de tribu, algún otro compañero y Alex Ureña

Inventario de software

14. ¿Conoce sobre la existencia de documentación relacionada a software con los que cuenta Xumtech? *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

15. ¿Utiliza su tribu algún inventario sobre software existente? (Si/no) *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

16. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría? *

Marca solo un óvalo.

- ◯ Con el líder de tribu
- ◯ Con el líder de tribu y Alex Ureña
- ◯ Solo con Alex Ureña
- ◯ Con el líder de tribu, algún otro compañero y Alex Ureña

Apéndice C – Plantilla de Revisión documental

Revisión documental

No. Revisión	
Fecha:	
Responsable	

Detalles del cambio	
Motivo de la revisión	
Fuente consultada	

Hallazgos	
No.	**Impacto**

Aprobación	
Estado	**Motivo**
Aprobado / Rechazado	

Firma: _____

Apéndice D – Minuta EM 03 – 0804

Minuta de reunión 03

Fecha:	08/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Si	
Katherine Matarrita	Si	

Temas tratados	
No.	**Tema**
1	Entrevista abierta sobre políticas de seguridad

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Firma de minuta	Sergio Arroyo	

Notas:

Para esta sesión, se planea realizar una entrevista abierta a Katherine Matarrita, colaboradora de Xumtech con el rol de Dueña de Producto. Se tocaron los siguientes temas:

Defensa Anti-Malware

1. Al ingresar a la empresa, ¿Alguien le mencionó temas relacionados al antivirus?
   La entrevistada menciona que no le mencionaron nada, pero que si es un tema que tenía pendiente consultar ya que su computadora da alertas de que el antivirus necesita ser reemplazado o actualizado.

2. Si Xumtech adquiere un antivirus, ¿Qué espera que la empresa le brinde para su uso?
   Espera un paso a paso de instalación, buenas prácticas cotidianas de uso. Además, menciona que se requiere que alguien dentro de la empresa esté especializado en el

tema para aclarar dudas de los equipos. Comenta que en la plataforma confluence debería centralizarse la información relacionada al antivirus.

3. ¿De contar con antivirus: ¿Qué gestiones realiza o realizaría con este?
   Revisaría el equipo periódicamente para evitar amenazas que pongan en riesgo su equipo y su información. Menciona que es la única función que conoce acerca del antivirus.

4. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
   Consultaría con Alex Ureña y con Margarita Ramos, esto debido a que Margarita es la líder de la tribu a la que pertenece.

Uso de keepass

1. ¿Ha usado usted la herramienta keepass?
   Comenta que si lo ha utilizado para consultar sobre contraseñas, pero que de momento no ha creado o actualizado algún registro.

2. ¿Sabe de la existencia de documentación relacionada al correcto uso de keepass?
   Comenta que desconoce si existe documentación, además, no ha consultado sobre la existencia de esta.

3. ¿Qué gestiones realiza con el keepass?
   De momento solo ha consultado registros.

4. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
   Lo consultaría con Zimri Zamora, colaboradora de la empresa que es su mentora de inducción. Además, elevaría la consulta con Alex Ureña.

Inventario de software

1. ¿Conoce a que herramientas tiene acceso en Xumtech?
   Menciona que las únicas que conoce son las que se le mencionaron el proceso de inducción por parte de la mentora Zimri Zamora.

2. ¿Conoce sobre la existencia de documentación relacionada a software con los que cuenta Xumtech?
   No sabe si existe documentación de este tipo.

3. De necesitar alguna aprobación/información relacionada a este tema, ¿Con cuáles personas lo consultaría?
   Menciona que le consultaría a Margarita Ramos por ser líder de la tribu o a Alex Ureña. Se inclina por personas que tienen más trayectoria profesional. Además, comenta que recientemente para instalar una herramienta tuvo que consultar a 4 personas; la cuarta persona fue la que le pudo dar información correcta acerca de la herramienta.

Apéndice E – Minuta EM 04 – 1804

Minuta de reunión 04

Fecha:	18/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Si	
Margarita Ramos Lopera	Si	

Temas tratados	
No.	**Tema**
1	Entrevista abierta sobre políticas de seguridad

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Firma de minuta	Sergio Arroyo	

Notas:

Para esta sesión, se planea realizar una entrevista abierta a Margarita Ramos Lopera, colaboradora de Xumtech con el rol de Dueña de Producto, además, se desempeña como líder de la "Tribu Maya", que es un equipo implementador de la empresa. Se tocaron los siguientes temas:

Defensa Anti-Malware

1. ¿Cuenta su equipo con antivirus (antimalware)?
   La entrevistada comenta que si tiene antivirus. Los criterios que utilizó para seleccionarlo están basados en criterios personales. El proyecto en el que está actualmente lo solicitaba como requisito.

2. ¿El cliente solicita criterios específicos para el antivirus?

Menciona que el requerimiento era únicamente tener un antivirus activo, actualizado y son sistema operativo actualizado. Lo que normalmente hace un antivirus.

3. ¿De contar con antivirus: ¿Qué gestiones realiza o realizaría con este?
   Menciona que comúnmente realiza análisis periódico del equipo y lo aplica semanalmente, lo actualiza cuando el antivirus se lo indica (generalmente una vez al mes)

4. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
   Por su rol, menciona que lo hace sola según la urgencia que tenga, pero generalmente de consultarlo con alguien lo hace con Alex Ureña.

5. ¿Aplica su tribu políticas de gestión de antivirus?
   Mneciona que en un momento se hicieron gestiones para gestionar esto cuando el cliente lo solicitó, pero que no se llegó a nada concreto, por tanto, de momento no se gestiona.

Uso de keepass

1. ¿Ha usado usted la herramienta keepass?
   Menciona que si lo utiliza de forma habitual.

2. ¿Sabe de la existencia de documentación relacionada al correcto uso de keepass?
   Menciona que en Confluence existe documentación relacionada al uso de Keepass.

3. ¿Sabe si su tribu conoce sobre la documentación disponible sobre el uso de keepass?
   Comenta que comúnmente les indica sobre la existencia de documentación importante en Confluence, pero específicamente sobre artículos relacionados al Keepass no les ha mencionado.

4. ¿Qué gestiones realiza con el keepass?
   Consulta usuarios, actualiza usuarios, sincroniza usuarios, consulta URL's de ambientes y, además, autogenera contraseñas con la herramienta.

5. De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
   Cualquier tema de este tipo los comenta con Alex Ureña o dependiendo del tema lo trataría con Hugo Brenes.

6. ¿Sabe si los miembros de su tribu aplican las reglas de uso de Keepass?
   No sabe si las aplican, pero, si ha notado que hay miembros que no están siguiendo las reglas.

Inventario de software

1. ¿Conoce sobre la existencia de documentación relacionada a software con los que cuenta Xumtech?
   No conoce la existencia sobre esto. Ella conoce porque muchos los ha usado.

2. ¿Utiliza su tribu algún inventario sobre software existente?
   Desconoce si su tribu utiliza esto.

3. De necesitar alguna aprobación/información relacionada a este tema, ¿Con cuáles personas lo consultaría?
   De requerir un sistema, ingresa a Keepass en donde hay información sobre herramientas. De no estar ahí, evalúa por su parte si lo necesita y lo adquiere por cuenta propia. Si le ve uso en la empresa lo conversa con algún alto mando para evaluar su uso y compra en toda la organización.

Apéndice F – Minuta EM 02 – 0504

Minuta de reunión 02

Fecha:	05/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Sí	
Alex Ureña	Sí	

Temas tratados	
No.	**Tema**
1	Selección de políticas de seguridad
2	Aprobación de inicio de encuestas y entrevistas

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Mostrar resultados obtenidos de las encuestas	Sergio Arroyo	Sin definir

Notas:

Para esta sesión, se presentó a Alex Ureña, contraparte de este proyecto y colaborador de Xumtech, la propuesta de políticas que se pretenden abarcar. Para esto se le mostró la lista propuesta por los controles CIS correspondiente al “Grupo de implementación 1”, que muestra controles válidos para empresas catalogadas como pequeñas. El entrevistado incluyó un tema que le parece relevante para su utilización en la empresa, dado el cambio al pasar a formar parte del régimen de zonas francas. La selección final de políticas corresponde a:

- Defensa contra software malicioso.
- Gestión de contraseñas basado en herramienta Keepass.
- Gestión de inventario de activos de software.

Apéndice G – Minuta RV 01 – 1504

Revisión documental

No. Revisión	1
Fecha:	15/04/2022
Responsable	Sergio Arroyo Torres

Detalles del cambio	
Motivo de la revisión	Verificar la existencia de documentación que permita identificar la existencia de procesos relacionados con el uso de Keepass en la organización.
Fuente consultada	Se consulta la página *Confluence,* la cual funciona como base de conocimiento de la organización.

Hallazgos	
No.	**Impacto**
1	Se valida que sí existe documentación relacionada con la gestión de Keepass en Confluence. El artículo lleva como nombre “Conectarse a la base de datos de credenciales con Keepass”
2	Al revisar el artículo es evidente la existencia de los procesos: Configuración inicial, consulta de usuarios, eliminar usuarios, actualización de usuarios y creación de usuarios.

Aprobación	
Estado	**Motivo**
Aprobado / Rechazado	**Aprobado**

Apéndice H – Minuta RV 02 – 1504

Revisión documental

No. Revisión	2
Fecha:	15/04/2022
Responsable	Sergio Arroyo Torres

Detalles del cambio	
Motivo de la revisión	Verificar la existencia de documentación que permita identificar la existencia de procesos relacionados con la gestión de antivirus en la organización.
Fuente consultada	Se consulta la página *Confluence*, la cual funciona como base de conocimiento de la organización.

Hallazgos	
No.	**Impacto**
1	Se valida que no existe documentación relacionada con la gestión de antivirus en *Confluence.*

Aprobación	
Estado	**Motivo**
Aprobado / Rechazado	**Aprobado**

Apéndice I – Minuta RV 03 – 1604

Revisión documental

No. Revisión	3
Fecha:	16/04/2022
Responsable	Sergio Arroyo Torres

Detalles del cambio	
Motivo de la revisión	Verificar la existencia de documentación que permita confirmar la existencia de procesos relacionados con la gestión de inventarios de activos de software en la organización.
Fuente consultada	Se consulta la página *Confluence,* la cual funciona como base de conocimiento de la organización.

Hallazgos	
No.	**Impacto**
1	Se valida que no existe documentación relacionada con la gestión de inventarios de activos de softwen *Confluence.*

Aprobación	
Estado	**Motivo**
Aprobado / Rechazado	**Aprobado**

Apéndice J – Conglomerado de datos recopilados de encuesta

Marca temporal	Nombre	Tribu	Puesto	¿Cuenta su equipo con antivirus (antimalware)?	¿Conoce usted si Xumtech cuenta con políticas de uso de antivirus?
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	Sí	No
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	Sí	No
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	No	No
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	No	No
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	Sí	No
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	No	No
4/12/2022 12:22:10	Sujeto 7	Tribu José	Consultor(a)	Sí	No
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	No	Si
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	No	No
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	Sí	No
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	Sí	No
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	No	No
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	No	No
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	No	No
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	Sí	No
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	No	No
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	Sí	No
4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	No	No

Marca temporal	Nombre	Tribu	Puesto	¿Qué gestiones realiza o realizaría con un antivirus? (Marque y/o agregue las opciones que considere correctas)	De necesitar alguna aprobación relacionada con este tema, ¿con cuáles personas lo consultaría?
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	Actualización automática o manual del antivirus	Con el líder de tribu y Alex Ureña
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	Análisis periódicos del equipo	Con el líder de tribu

4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros). Actualización automática o manual del antivirus.	Solo con Alex Ureña
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	Análisis de memorias externas (discos duros, memorias USB, otros).	Con el líder de tribu
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	Análisis periódicos del equipo	Con el líder de tribu
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	Actualización automática o manual del antivirus	Con el líder de tribu y Alex Ureña
4/12/2022 12:22:10	Sujeto 7	Tribu José	Consultor(a)	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros). Actualización automática o manual del antivirus.	Con el líder de tribu y Alex Ureña
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	No haría ninguna en particular, solo dejaría que el antivirus corra con normalidad	Con el líder de tribu
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	Análisis periódicos del equipo. Actualización automática o manual del antivirus.	Solo con Alex Ureña
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	Análisis periódicos del equipo. Actualización automática o manual del antivirus.	Con el líder de tribu y Alex Ureña
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	Análisis periódicos del equipo.	Con el líder de tribu

4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros). Revisar archivos descargados o archivos que envía el cliente por correo.	Con el líder de tribu
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	Análisis de memorias externas (discos duros, memorias USB, otros). Actualización automática o manual del antivirus.	Con el líder de tribu, algún otro compañero y Alex Ureña
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros).	Con el líder de tribu, algún otro compañero y Alex Ureña
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	Análisis periódicos del equipo. Actualización automática o manual del antivirus.	Con el líder de tribu
4/18/2022 9:33:23	Sujeto 16	Tribu Jose	Consultor(a)	Análisis periódicos del equipo. Actualización automática o manual del antivirus.	Solo con Alex Ureña
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros).	Con el líder de tribu

4/18/2022 9:45:43	Sujeto 18	Sujeto 18	Tribu Dunamis	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros). Actualización automática o manual del antivirus.	Con el líder de tribu
4/18/2022 9:50:58	Sujeto 19	Sujeto 19	Tribu Dunamis	Análisis periódicos del equipo. Análisis de memorias externas (discos duros, memorias USB, otros).	Con el líder de tribu y Alex Ureña
4/18/2022 10:07:18	Sujeto 20	Sujeto 20	Tribu Bulwak	Análisis periódicos del equipo, Actualización automática o manual del antivirus	Con el líder de tribu y Alex Ureña

Marca temporal	Nombre	Tribu	Puesto	¿Aplica su tribu políticas de gestión de antivirus?	¿Ha usado usted la herramienta keepass?
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	No	Sí
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	No	Sí
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	No	Sí
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	No	Sí
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	No	Sí
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	No	Sí
4/12/2022 12:22:10	Sujeto 7	Tribu Jose	Consultor(a)	No	Sí
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	No	Sí
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	No	Sí
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	No	Sí
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	No	Sí
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	No	Sí
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	No	Sí
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	No	Sí

4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	No	Sí
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	Sí	Sí
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	No	Sí
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	No	Sí
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	No	Sí
4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	No	Sí

Marca temporal	Nombre	Tribu	Puesto	¿Sabe de la existencia de documentación relacionada al correcto uso de keepass?	¿Utiliza su tribu reglas sobre el uso de keepass?
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	No	No
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	No	No
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	Si	Sí
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	Si	Sí
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	Si	Sí
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	Si	Sí
4/12/2022 12:22:10	Sujeto 7	Tribu José	Consultor(a)	Si	Sí
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	No	No
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	No	No
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	No	No
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	No	Sí
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	No	No
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	Si	Sí
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	No	No
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	Si	Sí
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	Si	Sí
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	Si	Sí
4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	Si	Sí

Marca temporal	Nombre	Tribu	Puesto	¿Qué gestiones realiza con el keepass? (Marque y/o agregue las opciones que considere correctas)	De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?

4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	Sincronización de usuarios	Con el líder de tribu
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	Consulta de usuarios. Agregar usuarios, Sincronización de usuarios.	Con el líder de tribu
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	Consulta de usuarios. Agregar usuarios. Eliminar usuarios. Sincronización de usuarios. Consulta de URLs de ambientes.	Solo con Alex Ureña
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	Consulta de usuarios. Sincronización de usuarios.	Con el líder de tribu
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	Consulta de usuarios. Agregar usuarios. Eliminar usuarios. Sincronización de usuarios.	Con el líder de tribu
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	Consulta de usuarios, Sincronización de usuarios	Con el líder de tribu, algún otro compañero y Alex Ureña
4/12/2022 12:22:10	Sujeto 7	Tribu Jose	Consultor(a)	Consulta de usuarios. Agregar usuarios.	Con el líder de tribu y Alex Ureña
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios. Ver/Agregar/Editar URLs de acceso a ambientes.	Con el líder de tribu
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Solo con Alex Ureña
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu

4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu, algún otro compañero y Alex Ureña
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu, algún otro compañero y Alex Ureña
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	Consulta de usuarios. Agregar usuarios.	Con el líder de tribu
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	Consulta de usuarios. Agregar usuarios. Eliminar usuarios. Sincronización de usuarios.	Con el líder de tribu y Alex Ureña
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	Consulta de usuarios. Agregar usuarios. Sincronización de usuarios.	Con el líder de tribu
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	Consulta de usuarios. Agregar usuarios. Eliminar usuarios. Sincronización de usuarios.	Con el líder de tribu y Alex Ureña

4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	Consulta de usuarios. Agregar usuarios. Eliminar usuarios. Sincronización de usuarios. Modificación de usuarios, específicamente actualización de contraseñas.	Con el líder de tribu

Marca temporal	Nombre	Tribu	Puesto	¿Conoce sobre la existencia de documentación relacionada a software con los que cuenta Xumtech?	¿Utiliza su tribu algún inventario sobre software existente? (Si/no)
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	No	No
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	No	No
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	No	No
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	Sí	Sí
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	No	No
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	Sí	Sí
4/12/2022 12:22:10	Sujeto 7	Tribu José	Consultor(a)	Sí	Sí
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	No	No
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	No	No
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	Sí	No
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	Sí	No
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	No	No
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	No	No
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	No	No
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	No	No
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	Sí	Sí
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	No	No
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	No	No
4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	No	No

Marca temporal	Nombre	Tribu	Puesto	De necesitar alguna aprobación relacionada a este tema, ¿Con cuáles personas lo consultaría?
4/12/2022 9:42:10	Sujeto 1	Tribu Onix	Consultor(a)	Con el líder de tribu
4/12/2022 9:45:12	Sujeto 2	Tribu Bulwak	Consultor(a)	Con el líder de tribu
4/12/2022 9:47:30	Sujeto 3	Tribu Onix	Líder técnico	Solo con Alex Ureña
4/12/2022 10:13:30	Sujeto 4	Tribu Maya	Consultor(a)	Con el líder de tribu
4/12/2022 10:20:13	Sujeto 5	Tribu Bulwak	Consultor(a)	Con el líder de tribu
4/12/2022 10:24:17	Sujeto 6	Tribu Maya	Consultor(a)	Con el líder de tribu y Alex Ureña
4/12/2022 12:22:10	Sujeto 7	Tribu José	Consultor(a)	Con el líder de tribu y Alex Ureña
4/12/2022 13:24:07	Sujeto 8	Tribu Bulwak	Líder técnico	Con el líder de tribu
4/12/2022 14:06:29	Sujeto 9	Tribu Andre	Líder técnico	Solo con Alex Ureña
4/12/2022 19:43:54	Sujeto 10	Tribu Bulwak	Consultor(a)	Con el líder de tribu y Alex Ureña
4/13/2022 10:05:41	Sujeto 11	Tribu Maya	Consultor(a)	Con el líder de tribu
4/18/2022 8:40:05	Sujeto 12	Tribu Onix	Consultor(a)	Con el líder de tribu
4/18/2022 8:49:17	Sujeto 13	Tribu Maya	Líder técnico	Con el líder de tribu
4/18/2022 8:49:37	Sujeto 14	Tribu Andre	Consultor(a)	Con el líder de tribu y Alex Ureña
4/18/2022 9:00:56	Sujeto 15	Tribu Alex	Consultor(a)	Con el líder de tribu
4/18/2022 9:33:23	Sujeto 16	Tribu José	Consultor(a)	Con el líder de tribu
4/18/2022 9:39:14	Sujeto 17	Tribu Dunamis	Consultor(a)	Con el líder de tribu
4/18/2022 9:45:43	Sujeto 18	Tribu Dunamis	Consultor(a)	Con el líder de tribu, algún otro compañero y Alex Ureña
4/18/2022 9:50:58	Sujeto 19	Tribu Dunamis	Líder técnico	Con el líder de tribu y Alex Ureña
4/18/2022 10:07:18	Sujeto 20	Tribu Bulwak	Consultor(a)	Con el líder de tribu y Alex Ureña

Apéndice K - Minuta EM 05 – 1606

Minuta de reunión 05

Fecha:	16/06/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Si	
Hugo Brenes	Si	

Temas tratados	
No.	**Tema**
1	Presentación de métricas y rubros para medición de oportunidades de mejora y efectividad en procesos.

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Firma de minuta	Sergio Arroyo	

Notas:

Se presenta a Hugo Brenes, colaborador de la organización, las métricas y rubros propuestos para la medición de Oportunidades de Mejora y Efectividad en los procesos.

Ante esto, Hugo Brenes señala que los rubros presentados se adaptan a la situación actual de la empresa, además, comenta que, de acuerdo con la naturaleza de las políticas de seguridad seleccionada también se adaptan de gran manera.

Hugo Brenes realiza recomendaciones asociadas a los cálculos de los rubros, en los cuáles realiza correcciones relacionadas a los cálculos mínimos de los rubros. Dichas recomendaciones se toman en cuenta y se realizan las correspondientes correcciones.

Apéndice L - Minuta EM 06 – 1706

Minuta de reunión 06

Fecha:	17/06/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Si	
Alex Ureña	Si	

Temas tratados	
No.	**Tema**
1	Presentación de actividades de procesos Cobit y su adaptación a Xumtech

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Firma de minuta	Sergio Arroyo	

Notas:

Se presenta a Alex Ureña las actividades que COBIT 5 recomienda para su aplicación en las políticas a ejecutar en el proyecto. Luego del análisis de cada una se toman los siguientes acuerdos:

Defensa contra software malicioso

Para la política de defensa contra software malicioso se plantearon a Alex Ureña las actividades recomendadas por COBIT 5 en el proceso “DSS05.01 Proteger contra Software malicioso (malware)”, así como las recomendadas a seguir por el estudiante y su cobertura mediante los procesos propuestos. Dado esto y según conversaciones con Alex Ureña, léase:

- Se excluye para el alcance de esta investigación la tercera actividad citada como “Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.” Lo anterior,

por cuanto según el entrevistado, la organización no posee la arquitectura tecnológica para seguir este tipo de recomendación.

- Se excluye de los procesos propuestos la quinta actividad citada por COBIT 5 como “Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de phishing)”. Alex Ureña menciona que, dada la naturaleza del negocio y la necesidad de estar en constante contacto con clientes y nuevas oportunidades de negocio, la organización no se encuentra en un nivel de madurez adecuado para implementar esta actividad.

Control y uso de privilegios administrativos

Para la política de control y uso de privilegios administrativos se presentaron al entrevistado de la organización, Alex Ureña, las actividades recomendadas por COBIT 5 en el proceso “DSS05.04 Gestionar la identidad del usuario y el acceso lógico”, así como lo planteado por el estudiante en los procesos propuestos. Según lo anterior, se define con el entrevistado que:

- Se descarta seguir la segunda actividad citada como “Identificar unívocamente todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio”. Lo anterior, dado que, según el entrevistado, el esquema del recurso humano de la organización no es lo suficientemente grande como para contar con distintas unidades de negocio, además, la empresa no posee roles funcionales definidos que se puedan utilizar en esta actividad.
- Dada la madurez de la organización en temas de estructura de recurso humano, actualmente no se cuenta con unidades de negocio por separado, así mismo, no existen distinciones en cuanto a clasificaciones de seguridad entre los distintos roles de la organización, por tanto, el entrevistado Alex Ureña señala que esta actividad se debe descartar para el alcance de este proyecto. La actividad se describe en lo siguiente: “Autenticar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación con aplicaciones usadas en procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente”.
- Para la quinta actividad, la cual señala que se deben “Segregar y gestionar cuentas de usuario privilegiadas”, el entrevistado señala que se debe descartar esta actividad, pues la información sobre la cual se crea este proceso es de libre acceso para todos los miembros de la organización, por tanto, no se necesitan accesos privilegiados.
- Para la octava actividad “Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible”, Alex Ureña señala que no aplica, pues, como se mencionó anteriormente, la información para la cual se crea este proceso no requiere de acceso privilegiado, porque es de acceso para toda la organización.

Inventario y control de los activos de software

Para la política de Inventario y control de los activos de software se presentaron a Alex Ureña los procesos previstos, así como las actividades propuestas por COBIT 5 para el proceso “BAI09.01 Identificar y registrar activos actuales” con lo cual se define lo siguiente:

- Se descarta la quinta actividad citada como “Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez”. Lo anterior, por cuanto, según el entrevistado, hasta este momento se contará con procesos establecidos para el registro de los activos, y al ser una empresa relativamente nueva, esta actividad puede cubrirse cuando la empresa tenga más madurez en este tema.
- El entrevistado Alex Ureña señala que se debe dejar de lado la cuarta actividad señalada como “Comprobar que los activos se adecuan a sus objetivos (p.ej., están en condiciones útiles)”. La poca madurez de este proceso en la organización hace que no existan objetivos definidos para los activos.

Propuesta de políticas de seguridad

2022

Contenido

Sobre este documento

Este documento tiene como objetivo presentar a la empresa Xumtech la propuesta de políticas de seguridad y sus procesos asociados, producto de la investigación realizada sobre la situación actual de la organización en cuanto a políticas de seguridad y la brecha identificada entre la situación actual y el marco de referencia COBIT 5.

Como parte del documento, se puede encontrar el detalle de cada uno de los procesos pertenecientes a las políticas, así como una explicación de lo que pretende abarcar cada política y cada uno de sus procesos. Además, se adjunta el análisis financiero de las políticas propuestas.

Rubros Xumtech para identificación de oportunidades de mejora

La oportunidad de mejora será evaluada con la escala definida en la Tabla 1. Rubros de evaluación de oportunidad de mejora. Cabe destacar que cada uno de estos rubros es una primera propuesta para la medición del término "Oportunidad de mejora", dado que en la literatura no existe un estándar o marco de referencia que brinde rubros a aplicar.

Cada uno de los rubros propuestos para Oportunidad de mejora fue seleccionado por las siguientes razones:

- Documentación existente: la importancia de la documentación que respalde una política radica en la posibilidad que tiene esta de ser replicado como conocimiento al resto de la organización. Una política no documentada puede provocar que se generen ambigüedades en su uso según el usuario que la aplique. Por tanto, una política sin documentar realmente suma porcentaje para ser identificada como una política con oportunidad de mejora. Este rubro representa un 50% del total debido a que la falta de documentación, sin duda alguna, es una de las principales razones de la gestión desarticulada de las políticas de seguridad en la organización.
- Aplicación en tribus: como ya se mencionó, la organización trabaja a partir de subgrupos denominados tribus. Como las políticas son de aplicación organizacional, es necesario conocer el nivel de arraigo que tiene una política en la organización, y este nivel de arraigo se debe interpretar como el número de tribus que aplican la política en sus funciones diarias. Este rubro representa un 35% del total dado que ayuda a medir que tan reconocida puede ser una política para los miembros pertenecientes a las tribus de la organización.
- Aprobaciones necesarias: el problema principal que se pretende abordar en esta investigación es la gestión desarticulada de la seguridad, por tanto, es necesario controlar el nivel de aprobaciones que pueden tener las políticas, esto con la finalidad de evitar que muten dependiendo de los colaboradores o roles que realicen aprobaciones relacionadas a las políticas. Este rubro cuenta con un porcentaje de 15% ya que, aunque es importante, no presenta el mismo peso que el resto de los rubros pueden tener para la gestión de las políticas.

Tabla 1. Rubros de evaluación de oportunidad de mejora

Oportunidades de mejora				
Rubro	Descripción del rubro	Valor	Opciones	
Documentación existente	La política cuenta o no con documentación que la respalde.	50%	No cuenta con documentación: 50%	Cuenta con documentación: 10%
Aprobaciones necesarias	Número de aprobaciones necesarias para la culminación del proceso.	15%	Requiere más de dos aprobaciones: 15%	Requiere dos o menos aprobaciones: 5%
Aplicación en tribus	Número de tribus que aplican la política.	35%	Se aplica en tres tribus o menos: 35%	Se aplica en más de tres tribus: 5%

Fuente: Elaboración propia, 2022.

Según la escala contenida en la Tabla 1. Rubros de evaluación de oportunidad de mejora, mientras mayor sea el porcentaje obtenido, mayor será considerada la política como candidata a oportunidad de mejora. Se considera que un 70% o más será considerado como una política con oportunidad de mejora alta, 50% o más será tomado como una oportunidad de mejora media, mientras que un porcentaje menor a 50% será tomado como una política con oportunidad de mejora baja. En la Tabla 2. Resumen porcentajes oportunidad de mejora se muestra los rangos de porcentajes obtenidos con su respectivo significado.

Tabla 2. Resumen porcentajes oportunidad de mejora

Porcentaje obtenido	Significado
Entre 70% y %100	Oportunidad de mejora alta
Entre 50% y 69%	Oportunidad de mejora media
Entre 20% y 49%	Oportunidad de mejora baja

Fuente: Elaboración propia, 2022.

Tabla 3. Rubros de evaluación de efectividad

Efectividad				
Rubro	Descripción del rubro	Valor	Opciones:	
Número de actores	Número de actores involucrados en la política	25%	Las personas involucradas en la política son mas de tres: 5%	Las personas involucradas en la política son tres o menos: 25%
Documentación existente	Existencia de documentación que soporte la política.	50%	La política no cuenta con documentación: 5%	La política cuenta con documentación: 50%
Aprobaciones necesarias	Mayor número de aprobaciones necesarias para la culminación de un proceso perteneciente a la política.	25%	Requiere más de dos aprobaciones: 5%	Requiere dos o menos aprobaciones: 25%

Fuente: Elaboración propia, 2022.

Según la Tabla 3. Rubros de evaluación de efectividad, mientras mayor sea el porcentaje obtenido por la política al ser evaluada, mayor será la efectividad de esta, por tanto, se considera que un porcentaje mayor a 75% será considerado como una política efectiva. Por otra parte, un porcentaje menor a 75% será considerado como una política carente de efectividad. En la Tabla 4. Resumen porcentajes efectividad se muestra el significado de los rubros de acuerdo con la suma de porcentajes obtenidos.

Tabla 4. Resumen porcentajes efectividad

Porcentaje obtenido	Significado
Entre 75% y %100	Política efectiva
Entre 15% y 74%	Política carente de efectividad

Fuente: Elaboración propia, 2022.

Rubros Xumtech para medición de efectividad de procesos

Por parte de la efectividad, esta será evaluada según la escala expuesta en la Tabla 3. Rubros de evaluación de efectividad y se tomaron en cuenta los siguientes rubros:

- Documentación existente: se debe considerar como parte fundamental de las políticas de seguridad la documentación existente sobre esta. Dicha documentación permite a las organizaciones establecer estrategias de difusión y comunicación de las buenas prácticas organizacionales para resguardar la seguridad. Este rubro representa un 50% del total debido a que la documentación es una de las principales herramientas para gestionar de forma articulada la seguridad, ya que al ser la misma documentación para toda la organización las tribus existentes se apegarán al mismo estándar.
- Número de actores: el total de colaboradores involucrados en la ejecución de una política de seguridad es de gran importancia debido a que al tratarse de aspectos de seguridad de la información se debe tener una ejecución rápida y poco burocrática. Este rubro representa un 25% del total del porcentaje y se iguala al rubro "Aprobaciones necesarias" debido a que ambos están estrictamente relacionados.
- Aprobaciones necesarias: como se mencionó anteriormente, para mantener la integridad y buen control sobre una política de seguridad es necesario que las aprobaciones involucradas en las políticas sean llevadas a cabo por un mismo rol, y que este rol sea el mismo independientemente de la tribu o colaborador que aplique una determinada política. Se determina que una política de seguridad de la información será efectiva si cuenta con un número reducido de aprobaciones. Este rubro representa un 25% del porcentaje total, ya que como se indicó anteriormente, está enlazado al rubro "Número de actores", que también tiene el mismo porcentaje.

Políticas y sus procesos

En esta sección se detallan los procesos que forman parte de cada una de las políticas de seguridad. Cabe destacar que cada proceso está adecuado a al marco de referencia COBIT 5

Control y uso de privilegios administrativos

Esta política tiene como principal objetivo englobar los procesos asociados a la gestión de los privilegios, accesos y usuarios con los que cuenta Xumtech. El desarrollo de cada uno de los procesos de esta política se llevó a cabo tomando como base la herramienta Keepass, la cual funciona como gestor de accesos institucional. Además, cada uno de los procesos está adaptado a lo dictaminado por el proceso DSS05.04 Gestionar la identidad del usuario y el acceso lógico del marco de referencia COBIT 5.

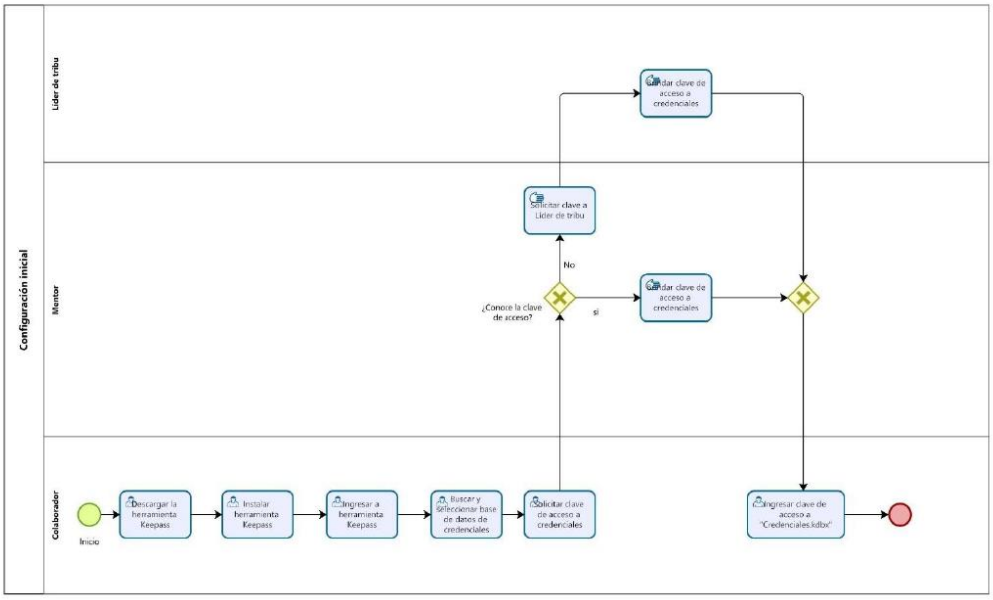
Configuración inicial

Este proceso tiene la finalidad de brindar guía sobre la configuración inicial que se debe llevar a cabo para utilizar la herramienta Keepass, la cual es utilizada por la organización como el gestor de los accesos y contraseñas. En la Ilustración 1. Proceso Configuración Inicial se muestra el diagrama del proceso especificado, el cual contiene las siguientes actividades:

- **Descargar la herramienta Keepass:** proceder con la descarga de la herramienta Keepass en el dispositivo brindado al colaborador.
- **Instalar herramienta Keepass:** instalar la herramienta Keepass, previamente descargada, en el correspondiente equipo.
- **Ingresar a herramienta Keepass:** ingresar a la herramienta Keepass, recientemente instalada.
- **Buscar y seleccionar base de datos de credenciales:** consiste en buscar el archivo al que accede Keepass para buscar los accesos de la organización. Dicho archivo se encuentra en el repositorio organizacional de documentos.
- **Solicitar clave de acceso a credenciales:** al seleccionar el archivo de credenciales, este solicita una contraseña. Dicha contraseña se debe solicitar al mentor, en primera instancia.

- **Solicitar clave a Líder de tribu:** si el mentor no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al líder de la tribu.
- **Brindar clave de acceso a credenciales:** el mentor, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- **Ingresar clave de acceso a "Credenciales.kdbx":** se ingresa la clave brindada para poder entrar a la herramienta y acceder a los accesos y contraseñas.

Ilustración 1. Proceso Configuración Inicial



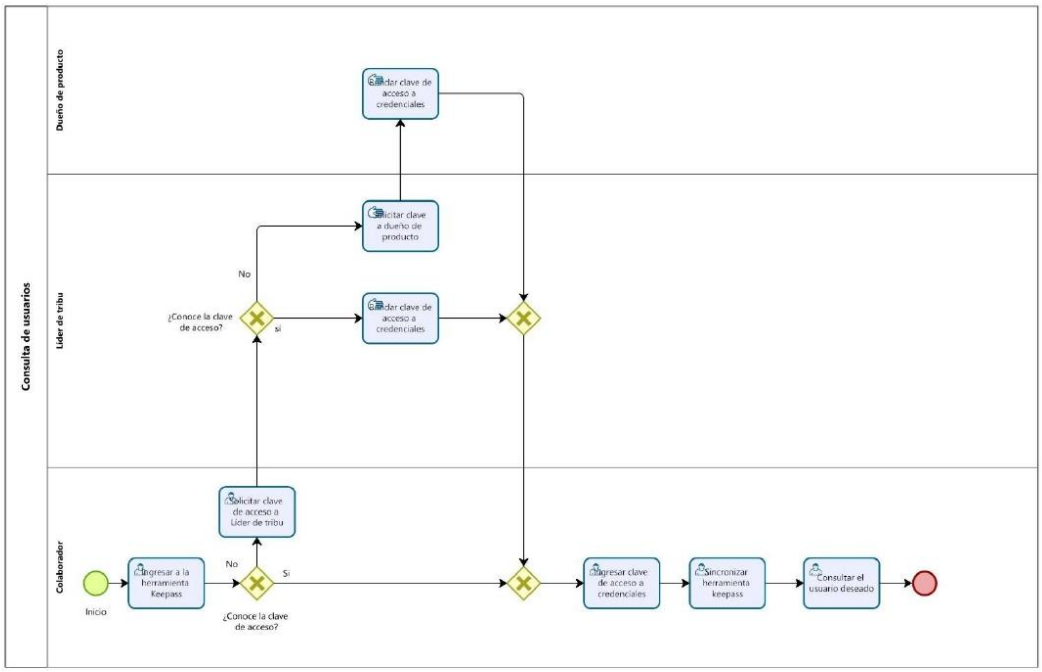
Fuente: Elaboración propia, 2022.

Consulta de usuarios

El principal objetivo de este proceso es determinar el paso a paso para consultar sobre un acceso o contraseña en la herramienta Keepass. En la Ilustración 2. Proceso Consulta de usuarios se puede visualizar el diagrama del proceso, el cual incluye las siguientes actividades:

- **Ingresar a herramienta Keepass:** ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.
- **Solicitar clave de acceso a Líder de tribu:** en caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- **Solicitar clave a dueño de producto:** si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al dueño de producto que corresponda.
- **Brindar clave de acceso a credenciales:** el dueño de producto, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- **Ingresar clave de acceso a credenciales:** se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- **Sincronizar herramienta Keepass:** tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- **Consultar el usuario deseado:** buscar entre los accesos y contraseñas existentes la que se necesite al momento la consulta.

Ilustración 2. Proceso Consulta de usuarios



Fuente: Elaboración propia, 2022.

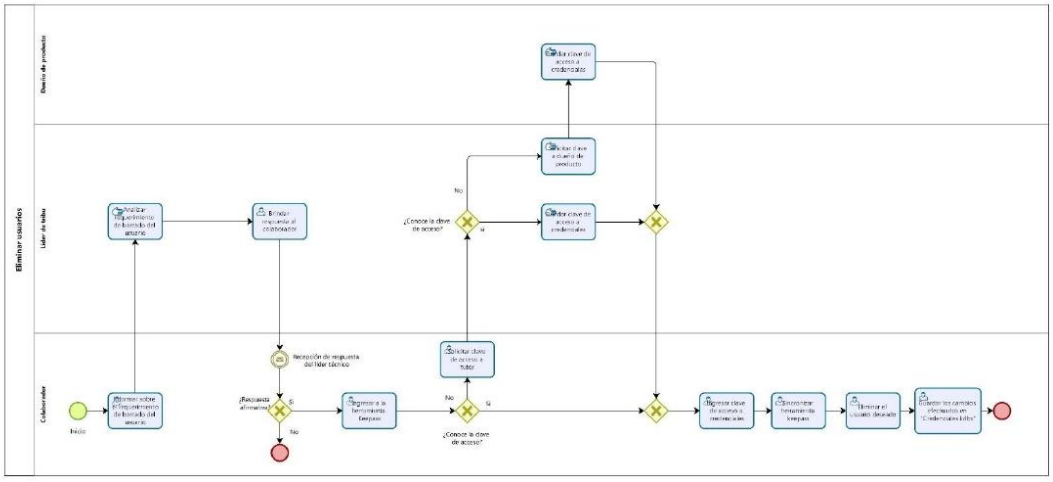
Eliminar usuarios

Proceso asociado a la política que se lleva a cabo para eliminar un usuario o acceso registrado en la herramienta Keepass. En la Ilustración 3. Proceso Eliminar Usuarios se muestra el proceso necesario para eliminar un usuario, en el cual se incluyen las siguientes actividades:

- **Informar sobre el requerimiento de borrado del usuario:** el colaborador debe informar al líder de tribu sobre el requerimiento y sus detalles.
- **Analizar requerimiento de borrado del usuario:** el líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesario eliminarlo o no.
- **Brindar respuesta al colaborador:** el líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.

- **Ingresar a herramienta Keepass:** ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.
- **Solicitar clave de acceso a Líder de tribu:** en caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- **Solicitar clave a dueño de producto:** si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al dueño de producto que corresponda.
- **Brindar clave de acceso a credenciales:** el dueño de producto, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- **Ingresar clave de acceso a credenciales:** se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- **Sincronizar herramienta Keepass:** tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- **Eliminar el usuario deseado:** el colaborador busca y elimina el determinado usuario.
- **Guardar los cambios efectuados en "Credenciales.kdbx":** el colaborador guarda los cambios en la herramienta, la cual actualiza el documento "Credenciales.kdbx".

Ilustración 3. Proceso Eliminar Usuarios



Fuente: Elaboración propia, 2022.

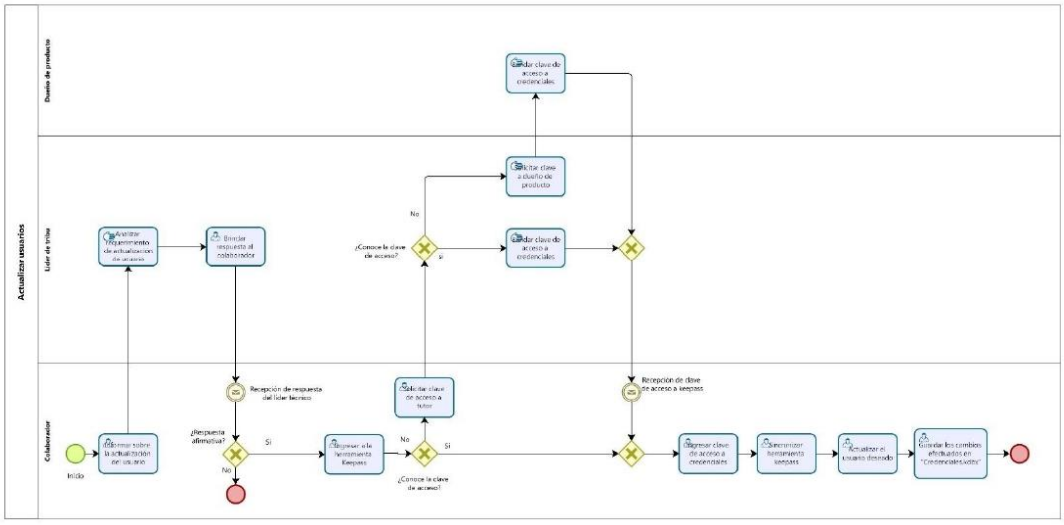
Actualizar usuarios

Este proceso contiene el conjunto de actividades necesario para actualizar un acceso o usuario registrado en la herramienta Keepass. En la Ilustración 4. Proceso Actualizar usuarios se encuentra el proceso necesario para llevar a cabo esta tarea, la cual incluye las siguientes actividades:

- **Informar sobre la actualización del usuario:** el colaborador debe informar al líder de tribu sobre el requerimiento y motivos por los cuales actualizar el usuario.
- **Analizar requerimiento de actualización de usuario:** el líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesaria la actualización.
- **Brindar respuesta al colaborador:** el líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.
- **Ingresar a herramienta Keepass:** ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.

- **Solicitar clave de acceso a Líder de tribu:** en caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- **Solicitar clave a dueño de producto:** si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al dueño de producto que corresponda.
- **Brindar clave de acceso a credenciales:** el dueño de producto, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- **Ingresar clave de acceso a credenciales:** se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- **Sincronizar herramienta Keepass:** tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- **Actualizar el usuario deseado:** el colaborador busca y actualiza el determinado usuario según lo que se requiera.
- **Guardar los cambios efectuados en "Credenciales.kdbx":** el colaborador guarda los cambios en la herramienta, la cual actualiza el documento "Credenciales.kdbx".

Ilustración 4. Proceso Actualizar usuarios



Fuente: Elaboración propia, 2022.

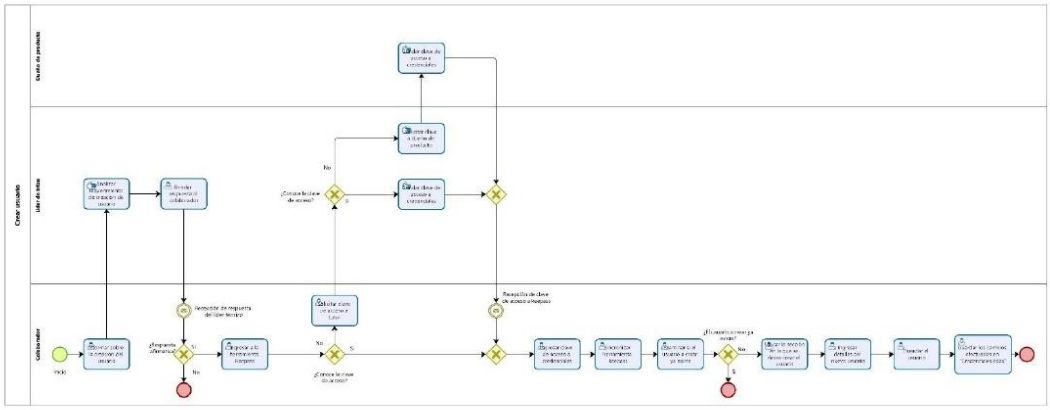
Crear Usuario

Proceso que se lleva a cabo para crear un usuario o acceso sobre la herramienta Keepass. En la Ilustración 5. Proceso Crear usuario se evidencian las actividades que se deben llevar a cabo para cumplir con este proceso, estas son:

- **Informar sobre la creación del usuario:** el colaborador debe informar al líder de tribu sobre el requerimiento y motivos por los cuales crear el usuario.
- **Analizar requerimiento de creación del usuario:** el líder de tribu analiza el requerimiento otorgado por el colaborador y determina si es necesaria la creación del usuario.
- **Brindar respuesta al colaborador:** el líder de tribu brinda respuesta al colaborador sobre la decisión tomada acerca del requerimiento.
- **Ingresar a herramienta Keepass:** ingresar a la herramienta Keepass, la cual se encuentra instalada en el equipo.
- **Solicitar clave de acceso a Líder de tribu:** en caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.

- **Solicitar clave a dueño de producto:** si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al dueño de producto que corresponda.
- **Brindar clave de acceso a credenciales:** el dueño de producto, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.
- **Ingresar clave de acceso a credenciales:** se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- **Sincronizar herramienta Keepass:** tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- **Examinar si el usuario a crear ya existe:** el colaborador que desea crear el usuario revisa la herramienta Keepass para determinar si el usuario ya existe o no.
- **Ubicar la sección en la que se desea crear el usuario:** el colaborador revisa la estructura creada y determina en que sección se debe crear el usuario.
- **Ingresar detalles del nuevo usuario:** el colaborador ingresa los detalles del usuario a crear, según corresponda.
- **Guardar el usuario:** guardar en la herramienta los detalles del usuario creado.
- **Guardar los cambios efectuados en "Credenciales.kdbx":** el colaborador guarda los cambios en la herramienta, la cual actualiza el documento "Credenciales.kdbx".

Ilustración 5. Proceso Crear usuario



Fuente: Elaboración propia, 2022.

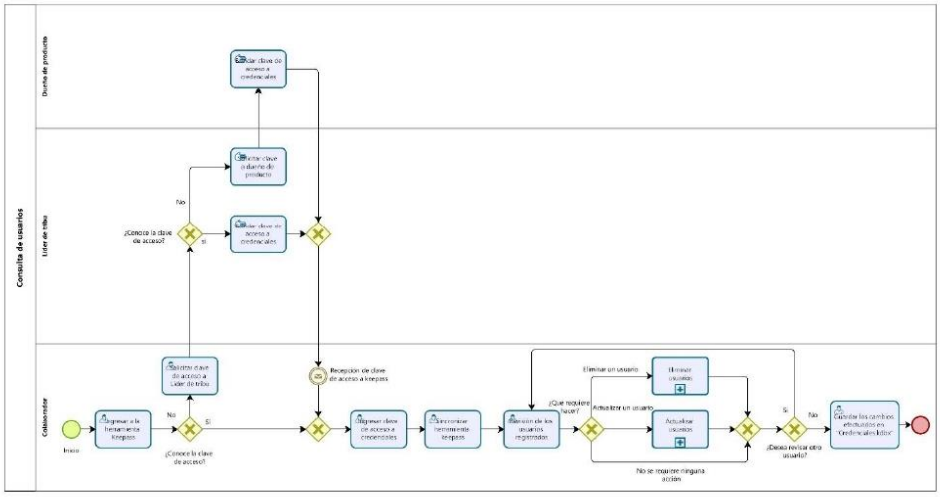
Revisión de usuarios

Este proceso se lleva a cabo con el objetivo de realizar una revisión sobre los usuarios existentes, esto con el fin de depurar la base de datos de accesos existente. En la Ilustración 6. Proceso Revisión de usuarios se muestra el diagrama del proceso, así como las actividades que se deben llevar a cabo para su cumplimiento. Entre las actividades se encuentran:

- **Ingresar a la herramienta Keepass:** el colaborador ingresa a la herramienta Keepass, instalada en el equipo.
- **Solicitar clave de acceso a Líder de tribu:** en caso de no conocer la clave de acceso, esta debe ser solicitada al líder de la tribu a la cual pertenezca.
- **Solicitar clave a dueño de producto:** si el líder de tribu no conoce la clave de acceso a las credenciales, este debe solicitar la clave de acceso al dueño de producto que corresponda.
- **Brindar clave de acceso a credenciales:** el dueño de producto, o líder de tribu deben brindar la contraseña de acceso a las credenciales. Esta debe brindarse por medio de chat y no debe ser escrita en algún archivo o correo electrónico.

- **Ingresar clave de acceso a credenciales:** se ingresa la clave brindada para poder entrar a la herramienta y visualizar los accesos y contraseñas.
- **Sincronizar herramienta Keepass:** tarea que se lleva a cabo para actualizar los accesos y contraseñas a la última versión guardada por otro usuario.
- **Revisión de los usuarios registrados:** el colaborador a cargo de la tarea revisa los usuarios existentes, para validar si se requiere eliminar o actualizar un usuario.
- **Actualizar usuarios (subproceso):** si es requerido en la revisión, el usuario ejecuta el proceso de actualizar un usuario.
- **Eliminar usuarios (subproceso):** si es requerido producto de la revisión, el usuario puede ejecutar el proceso de eliminar un usuario.
- **Guardar los cambios efectuados en "Credenciales.kdbx":** el colaborador guarda los cambios en la herramienta, la cual actualiza el documento "Credenciales.kdbx".

Ilustración 6. Proceso Revisión de usuarios



Fuente: Elaboración propia, 2022.

Defensa contra software malicioso

Esta política tiene como principal objetivo englobar los procesos asociados al correcto uso del antivirus institucional, en aras de proteger los activos tangibles e intangibles de la empresa Xumtech.

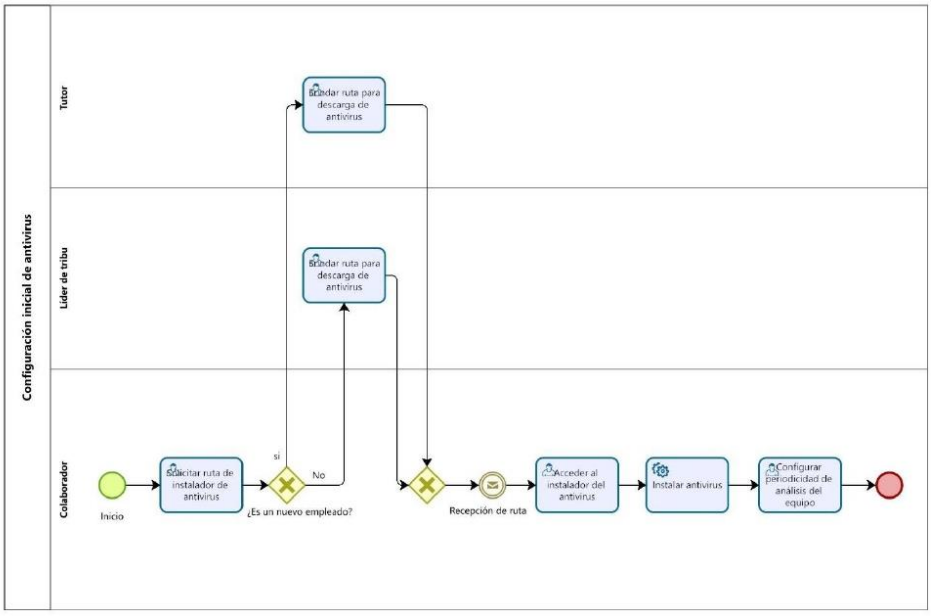
El desarrollo de cada uno de los procesos de esta política se llevó a cabo tomando como base el proceso DSS05.01 Proteger contra Software malicioso (malware) del marco de referencia COBIT 5. Esta política se llevó a cabo sin conocimiento de cual será la herramienta anti-malware de la organización, pero establecida de forma general y basada en las buenas prácticas para que pueda ser ejecutada independientemente del antivirus que se elija.

Configuración inicial de antivirus

Este proceso tiene como principal objetivo ser una guía de configuración para los colaboradores que deseen instalar en sus equipos el antivirus de la organización. En la Ilustración 7. Proceso Configuración inicial de antivirus se muestra el diagrama del proceso, el cual cuenta con las siguientes actividades:

- **Solicitar ruta de instalador de antivirus:** el colaborador solicita la ruta de la cual debe descargar el instalador del antivirus.
- **Brindar ruta para descarga de antivirus:** el tutor o el líder de la tribu brindan la ruta de la cual el colaborador puede descargar el instalador del antivirus. Si se trata de un nuevo empleado, la ruta la brindará el mentor del nuevo colaborador, de lo contrario, deberá ser brindada por el líder de la tribu.
- **Acceder al instalador de antivirus:** el colaborador accede al instalador según la ruta que le fue brindada.
- **Instalar antivirus:** el colaborador ejecuta las acciones necesarias para que la instalación del antivirus sea efectiva.
- **Configurar periodicidad de análisis del equipo:** el colaborador configura que tan seguido se hará la revisión automática del equipo.

Ilustración 7. Proceso Configuración inicial de antivirus



Fuente: Elaboración propia, 2022.

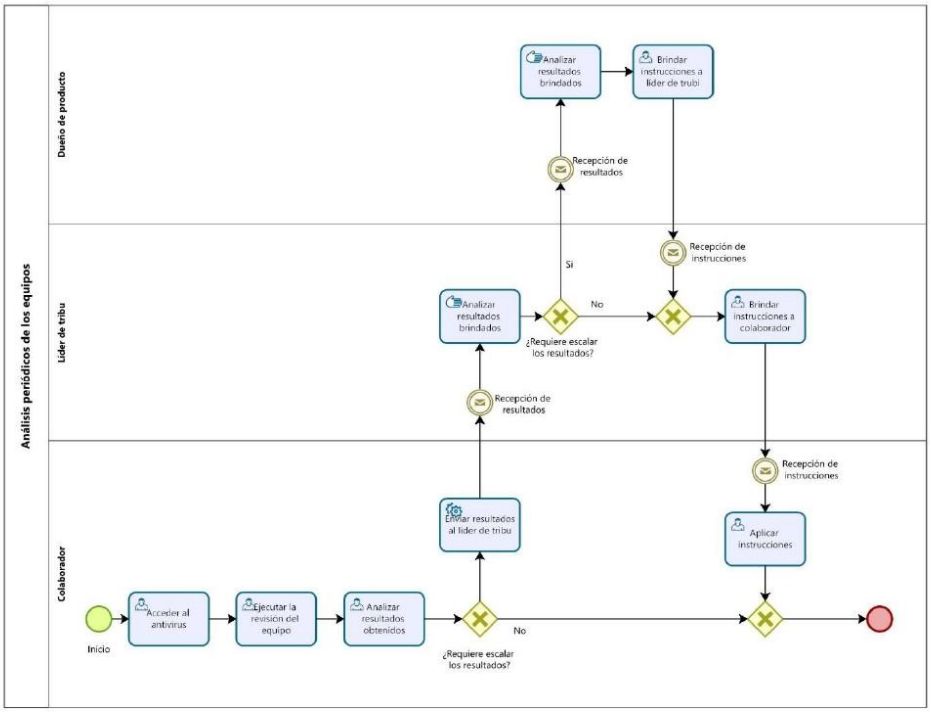
Análisis periódicos de los equipos

Este proceso menciona los pasos que el colaborador debe llevar a cabo cuando realice el análisis del equipo mediante el antivirus y según los resultados que este análisis arroje. En la Ilustración 8. Proceso Análisis periódicos de los equipos se muestra el diagrama asociado al proceso mencionado. Este proceso cuenta con las siguientes actividades:

- **Acceder al antivirus:** el colaborador accede a la herramienta de antivirus instalada en su equipo.
- **Ejecutar la revisión del equipo:** el colaborador ejecuta la funcionalidad del antivirus que analiza el equipo y todos los archivos que en este se encuentran.

- **Analizar resultados obtenidos:** el colaborador analiza los resultados arrojados por la herramienta para determinar si estos requieren ser escalados o no.
- **Enviar resultados al líder de tribu:** el colaborador envía, de ser necesario, los resultados obtenidos para que el líder de tribu valide si ponen en riesgo información o equipos pertenecientes a la tribu.
- **Analizar los resultados brindados:** el líder de tribu, o el dueño de producto evalúan los resultados aportados por el colaborador, esto para determinar las acciones correctivas a llevar a cabo.
- **Brindar instrucciones a colaborador:** el líder de tribu, o el dueño de producto, brindan retroalimentación al colaborador sobre las acciones a llevar a cabo.
- **Aplicar instrucciones:** el colaborador aplica las instrucciones brindadas por el líder de la tribu o por el dueño de producto.

Ilustración 8. Proceso Análisis periódicos de los equipos



Fuente: Elaboración propia, 2022.

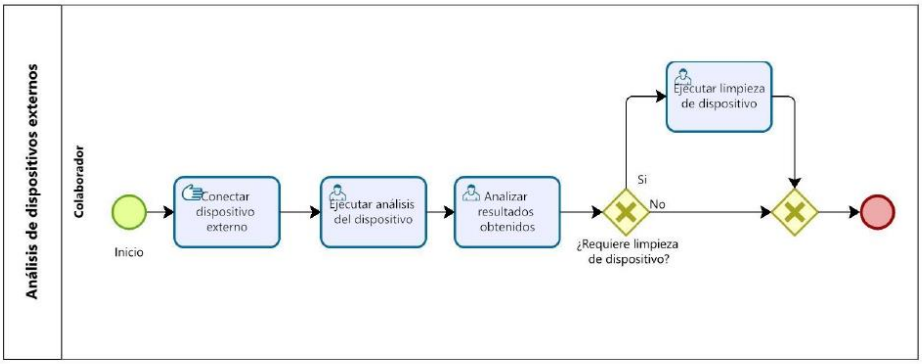
Análisis de dispositivos externos

Este proceso brinda el paso a paso que debe seguir un colaborador para ejecutar el análisis de algún dispositivo externo propio que conecte a un equipo de la organización. En la Ilustración 9. Proceso Análisis de dispositivos externos se evidencia el diagrama asociado a dicho proceso, el cual contiene las siguientes actividades:

- **Conectar dispositivo externo:** el colaborador conecta al equipo el dispositivo externo.
- **Ejecutar análisis del dispositivo:** antes de ingresar al dispositivo, el colaborador ejecuta el análisis de amenazas que provee el antivirus.

- **Analizar resultados obtenidos:** el colaborador analiza los resultados que arroja el antivirus, esto para determinar si es fiable ingresar o no.
- **Ejecutar limpieza de dispositivo:** de ser requerido, el colaborador se encargará de ejecutar la limpieza del dispositivo para eliminar cualquier tipo de amenazas.

Ilustración 9. Proceso Análisis de dispositivos externos



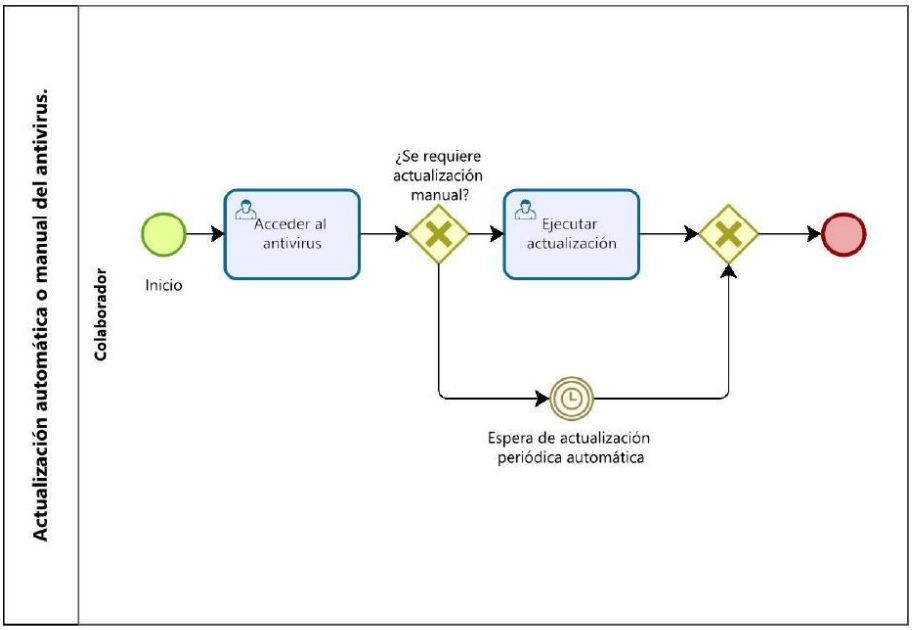
Fuente: Elaboración propia, 2022.

Actualización automática o manual del antivirus

Este proceso muestra las actividades necesarias para que el antivirus se actualice de forma manual o automática. En la Ilustración 10. Proceso Actualización automática o manual del antivirus se puede visualizar el proceso de ejecución paso a paso, el cual cuenta con las siguientes actividades:

- **Acceder al antivirus:** el colaborador accede a la herramienta de antivirus instalada en su equipo.
- **Ejecutar actualización:** de ser requerido, el colaborador puede ejecutar la actualización manual del antivirus.

Ilustración 10. Proceso Actualización automática o manual del antivirus



Fuente: Elaboración propia, 2022.

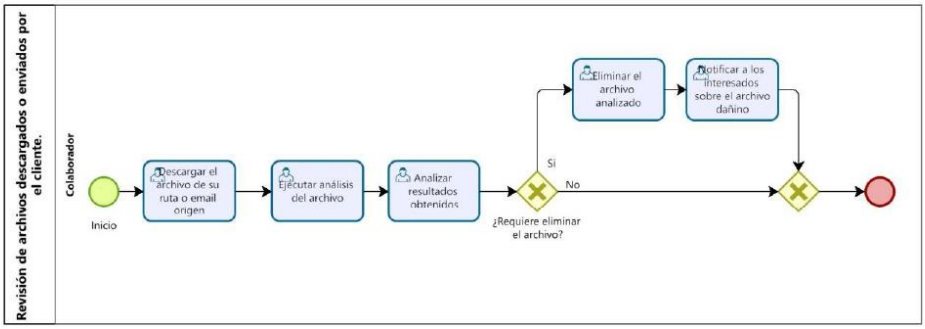
Revisión de archivos descargados o enviados por el cliente

Con el fin de evitar cualquier tipo de amenaza proveniente de archivos descargados de internet o enviados por el cliente, este proceso muestra el paso a paso a seguir para analizar dichos archivos. En la Ilustración 11. Proceso Revisión de archivos descargados o enviados por el cliente se incluye el diagrama del proceso. Este cuenta con las siguientes actividades:

- **Descargar el archivo de su ruta o email origen:** el colaborador descarga en el equipo el archivo que desea utilizar, ya sea de internet o de la fuente aportada por el cliente.
- **Ejecutar el análisis del archivo:** utilizando el antivirus, el colaborador ejecuta el análisis de los archivos descargados.
- **Analizar resultados obtenidos:** según lo arrojado por el antivirus, el colaborador analiza dichos resultados obtenidos.

- **Eliminar el archivo analizado:** el colaborador borra del equipo el archivo analizado debido a algún riesgo arrojado por el antivirus.
- **Notificar a los interesados sobre el archivo dañino:** se debe comunicar a los interesados de la organización sobre el borrado del archivo. Así mismo, se debe notificar al cliente, en caso de ser necesario, para que tome acciones preventivas.

Ilustración 11. Proceso Revisión de archivos descargados o enviados por el cliente



Fuente: Elaboración propia, 2022.

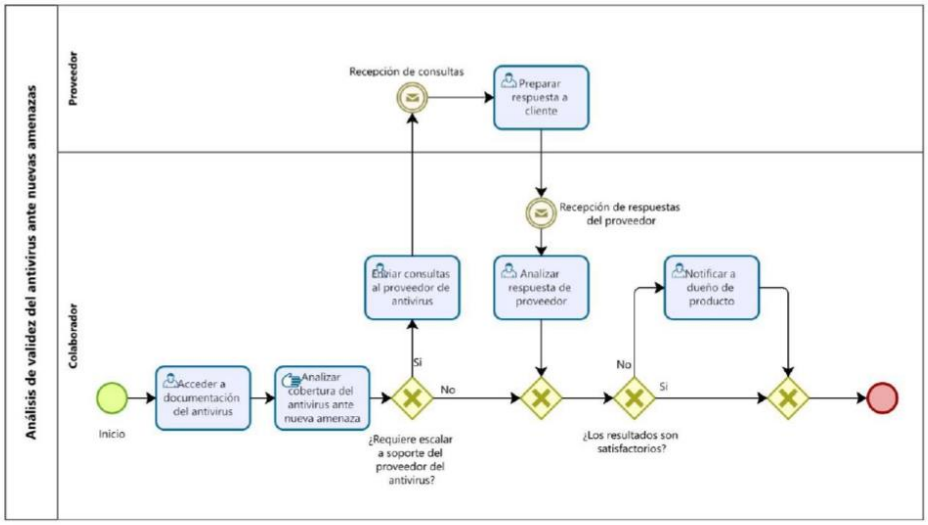
Análisis de validez del antivirus ante nuevas amenazas

Con el fin de determinar si el antivirus aún cubre a la organización contra nuevas amenazas, este proceso incluye todas las actividades necesarias para dicho análisis. En la Ilustración 12. Proceso Análisis de validez del antivirus ante nuevas amenazas se muestra el diagrama asociado al proceso. Este diagrama incluye las siguientes actividades:

- **Acceder a documentación del antivirus:** el colaborador accede a la documentación aportada por el proveedor del antivirus.
- **Analizar cobertura del antivirus ante nueva amenaza:** el colaborador analiza si el antivirus ofrece protección a la organización sobre la nueva amenaza a investigar.
- **Enviar consultas al proveedor de antivirus:** el colaborador prepara y envía las consultas al proveedor del servicio, en caso de ser necesario.

- **Preparar respuesta a cliente:** el proveedor debe dar respuesta a las consultas de la organización.
- **Analizar respuesta de proveedor:** el colaborador analiza las respuestas aportadas por el proveedor y analiza si requiere escalarlo al dueño de producto necesario.
- **Notificar a dueño de producto:** de ser necesario, el colaborador puede escalar al dueño de producto la situación ocurrida con el antivirus.

Ilustración 12. Proceso Análisis de validez del antivirus ante nuevas amenazas



Fuente: Elaboración propia, 2022.

Inventario y control de los activos de software

Esta política tiene como principal objetivo englobar los procesos asociados a la gestión de los activos de software de la empresa Xumtech.

El desarrollo de cada uno de los procesos de esta política se llevó a cabo tomando como base el proceso BAI09.01 Identificar y registrar activos actuales del marco de referencia COBIT 5.

En los procesos pertenecientes a esta política se utiliza la plataforma "Confluence", la cual es utilizada por la empresa Xumtech como repositorio de conocimiento organizacional.

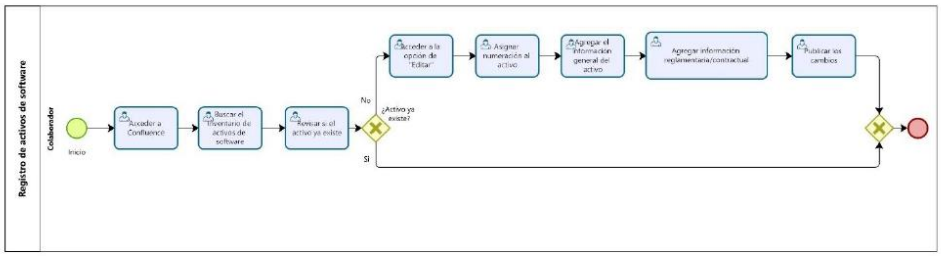
A continuación, se detallan los procesos pertenecientes a esta política, así como los diagramas *To-be* pertenecientes a cada proceso.

Registro de activos de software

Este proceso tiene como finalidad brindar claridad sobre como registrar un activo de software sobre el inventario existente en la organización. Cabe destacar que dicho inventario se encuentra en la herramienta Confluence, detallada en XX, y la cual funciona como repositorio de conocimiento de la organización. En la Ilustración 13. Proceso Registro de activos de software se muestra el diagrama asociado al proceso, el cual cuenta con las siguientes actividades:

- **Acceder a Confluence:** el colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- **Buscar el inventario de activos de software:** al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- **Revisar si el activo ya existe:** el colaborador revisa y verifica que en el inventario no exista el activo de software a registrar.
- **Acceder a la opción de "Editar":** para poder editar el inventario, el colaborador debe acceder a la opción de "Editar".
- **Asignar numeración al activo:** al ingresar el activo, el colaborador revisa la numeración existente con el fin de asignar un número único.
- **Agregar información reglamentaria/contractual:** agregar a la línea del activo la información reglamentaria y contractual que corresponda al activo de software.
- **Publicar los cambios:** una vez ingresada toda la información relacionada al activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 13. Proceso Registro de activos de software



Fuente: Elaboración propia, 2022.

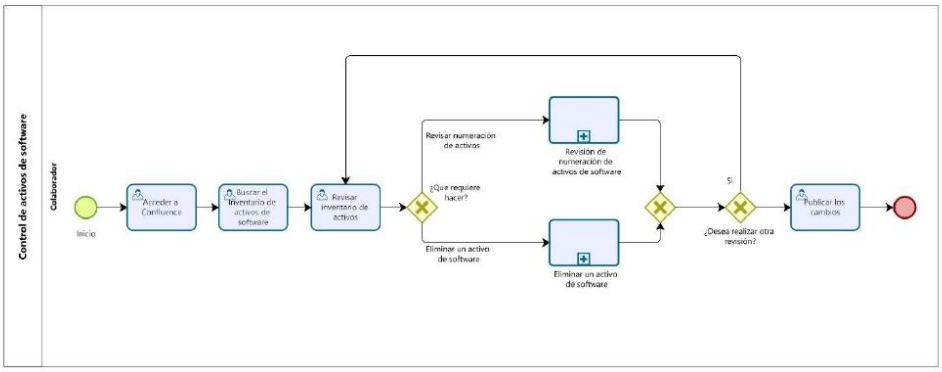
Control de activos de software

Este proceso tiene la finalidad de establecer revisiones sobre el inventario de activos de software para determinar si se requiere eliminar o enumerar alguno de los ya registrados. En la Ilustración 14. Proceso Control de activos de software se muestra el diagrama asociado al proceso. Las actividades de este proceso son:

- **Acceder a Confluence:** el colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- **Buscar el inventario de activos de software:** al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- **Revisar inventario de activos:** el colaborador revisa el inventario con el fin de determinar si se requiere actualizar alguno de los ya existentes.
- **Revisión de numeración de activos de software (subproceso):** si fuera necesario, el colaborador puede ejecutar el proceso de numeración de activos de software producto de la revisión que haya realizado. Este proceso asigna numeración única a los activos de software.
- **Eliminar un activo de software (subproceso):** si fuera necesario, el colaborador puede ejecutar el proceso de eliminar un activo de software, esto producto de la revisión que haya realizado y de los resultados que haya obtenido.

- **Publicar los cambios:** una vez ingresada toda la información relacionada al activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 14. Proceso Control de activos de software



Fuente: Elaboración propia, 2022.

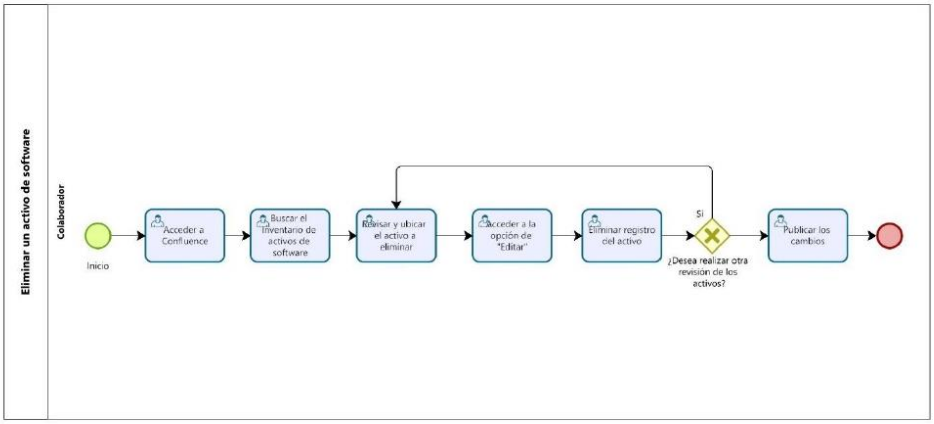
Eliminar un activo de software

Este proceso se lleva a cabo cuando sea necesario borrar un activo de software existente en el inventario. En la Ilustración 15. Proceso Eliminar un activo de software se detalla el diagrama del proceso. Este cuenta con las siguientes actividades:

- **Acceder a Confluence:** el colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- **Buscar el inventario de activos de software:** al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- **Revisar y ubicar el activo a eliminar:** una vez ingresado en el inventario, el colaborador debe ubicar el activo a eliminar.
- **Acceder a la opción de "Editar":** para poder editar el inventario, el colaborador debe acceder a la opción de "Editar".

- **Eliminar el registro del activo:** al ubicarlo, el colaborador debe eliminar todos los datos asociados al activo de software.
- **Publicar los cambios:** una vez ingresada toda la información relacionada al activo, el colaborador debe publicar los cambios para que se vean reflejados en el inventario.

Ilustración 15. Proceso Eliminar un activo de software



Fuente: Elaboración propia, 2022.

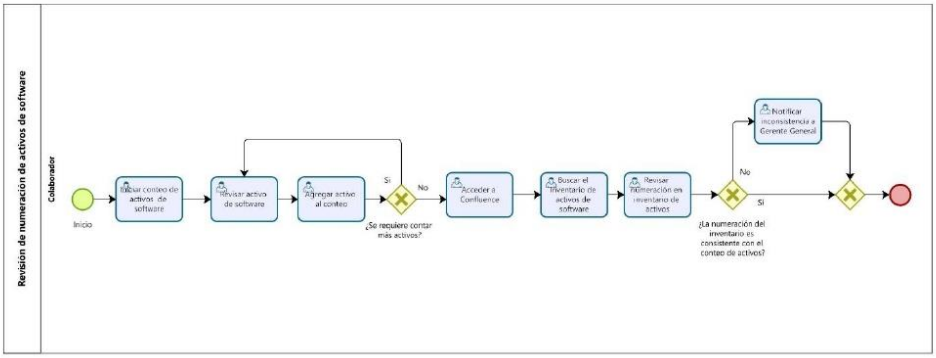
Revisión de numeración de activos de software

Este proceso tiene como objetivo asignar a cada activo de software un número de identificación específico, lo que permite ubicarlo a él y sus detalles contractuales y reglamentarios en el inventario. En la Ilustración 16. Proceso Revisión de numeración de activos de software se detalla el proceso que se lleva a cabo para la enumeración, además, este proceso cuenta con las actividades:

- **Iniciar conteo de activos de software:** el colaborador revisa los activos de software y verifica que el número de activos existente corresponde a los registrados en el inventario.
- **Revisar activo de software:** el colaborador revisa que el activo de software a contar se encuentra en el inventario.

- **Agregar activo al conteo:** si el conteo va bien, el colaborador agrega el activo de software al conteo del inventario.
- **Acceder a Confluence:** el colaborador debe acceder a Confluence con el usuario y contraseña asignado por la organización.
- **Buscar el inventario de activos de software:** al ingresar con sus credenciales, el colaborador debe buscar en Confluence el inventario de activos de software.
- **Revisar numeración en inventario de activos:** el colaborador revisa que la numeración realizada corresponda con la registrada en el inventario.
- **Notificar inconsistencia al Gerente General:** de ser necesario, el colaborador puede informar al Gerente General sobre alguna inconsistencia existente sobre el inventario de los activos de software.

Ilustración 16. Proceso Revisión de numeración de activos de software



Fuente: Elaboración propia, 2022.

Tabla 5. Salario investigador

Salario mínimo licenciatura universitaria	
Mensual	¢892.476,42
Semanal	¢223.119,105
Diario	¢44.623,82
Hora	¢5577,98

Fuente: Elaboración propia, 2022.

3.1.1.1 Control y uso de privilegios administrativos

Para el análisis financiero de esta política es necesario tomar en cuenta los análisis de recursos realizados sobre los procesos *As-Is* y los procesos *To-be*. En la Tabla 6. Costo total política Control y uso de privilegios administrativos As-Is y la Tabla 7. Costo total política Control y uso de privilegios administrativos To-be se establecen los costos relacionados a la ejecución de 40 corridas a los procesos por día, para un periodo de un mes.

Tabla 6. Costo total política Control y uso de privilegios administrativos As-Is

Proceso	Costo
Configuración Inicial	6.933.358,69
Crear Usuario	5.713.715,19
Consulta de usuarios	2.666.868,40
Eliminar usuarios	3.635.741,12
Actualización de usuarios	3.458.910,00
Total	22.408.593,40

Fuente: Elaboración propia, 2022.

Tabla 7. Costo total política Control y uso de privilegios administrativos To-be

Proceso	Costo
Configuración Inicial	6.933.358,69
Crear Usuario	1.378.079,66
Consulta de usuarios	2.666.868,40

Análisis financiero

Para determinar la viabilidad financiera de las políticas de seguridad propuestas se utiliza la métrica denominada Retorno de la inversión (ROI, por sus siglas en inglés). Esta métrica es usada para determinar la ganancia de una empresa sobre una determinada inversión realizada, por tanto, con esta métrica se puede determinar si una inversión vale la pena o no. Para el cálculo del retorno de inversión se utiliza la fórmula que se muestra en la Ilustración 17. Fórmula ROI.

Ilustración 17. Fórmula ROI

$$\frac{\text{Ganancia} - \text{Inversión}}{\text{Inversión}}$$

Fuente: Elaboración propia, 2022.

Para determinar el retorno de inversión de las políticas, es necesario conocer el monto total en inventario de las computadoras laptops que utilizan los colaboradores, por tanto, se tomará un valor de ₡20.000.000, significando esto una valoración de ₡500.000 por equipo.

Además, con el fin de poder calcular el monto relacionado al colaborador que realiza la investigación, se utilizará como base el salario mínimo establecido por el Ministerio de Trabajo de Costa Rica, el cual según MTSS (2022) es de ¢705.514,95 mensuales para el segundo semestre del 2022. A este monto, se le debe agregar el monto de cargas sociales, el cual corresponde a 26.5% sobre el total. Para determinar el monto final de salario, se debe realizar el siguiente cálculo:

¢705.514,95 * 1.265 = ¢892.476,42

En la Tabla 5. Salario investigador se muestra el detalle de los montos utilizados como salario base.

Eliminar usuarios	1.719.882,55
Actualización de usuarios	1.598.004,94
Revisión de usuarios	8.785.640,38
Total	23.081.834,62

Fuente: Elaboración propia, 2022.

Siendo así, al aplicar la métrica *ROI* se definen las siguientes premisas:

- Para el cálculo de la ganancia se debe determinar la diferencia entre el costo total del escenario *As-Is,* detallado en la Tabla 6. Costo total política Control y uso de privilegios administrativos As-Is, y el costo total del escenario *To-be* expuesto en la Tabla 7. Costo total política Control y uso de privilegios administrativos To-be. Al realizar el cálculo mencionado, se obtiene el siguiente resultado:

  ₡22.408.593,40 - ₡23.081.834,62 = -₡673.241,22

  En conclusión, el resultado total de la ganancia es de -₡673.241,22.
- Para la inversión, es necesario contabilizar las dieciséis semanas en las que el investigador desarrolló la propuesta de políticas y sus determinados procesos. En la Tabla 5. Salario investigador se muestra el costo relacionado con el investigador en distintas medidas de tiempo. Para el intervalo semanal, el costo asociado es de ¢223.119,105, además, la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado con lo anteriormente mencionado sería el siguiente:

  ¢223.119,105 * 16 = ¢3.569.905,68

  Por tanto, el costo total de la inversión es de ¢3.569.905,68

Por tanto, y para brindar el resultado asociado a la métrica *ROI* descrita en la Ilustración 17. Fórmula ROI, y tomando en cuenta la ganancia e inversión descritas anteriormente, el cálculo se realiza según lo mostrado en la Ilustración 18. Cálculo ROI Control y uso de privilegios administrativos.

Ilustración 18. Cálculo ROI Control y uso de privilegios administrativos

$$\frac{-₡673.241,22 - ¢3.569.905,68}{¢3.569.905,68} = -1.18$$

Fuente: Elaboración propia, 2022

Según lo mostrado en la Ilustración 18. Cálculo ROI Control y uso de privilegios administrativos se determina que el retorno de la inversión es el resultante del cálculo:

-1.18 * 100 = -118%

Como se evidencia, el retorno de la inversión es negativo, lo cual significa que para esta política la inversión está generando pérdida. Sin embargo, es importante aclarar que este era un resultado esperado, ya que la versión *To-be* de la política incluye actividades y procesos extra con el fin de cumplir con el marco de referencia COBIT 5. Es importante destacar que, dada la naturaleza del proyecto, el retorno de la inversión no es una métrica decisiva para medir el éxito del proyecto, ya que el propósito de dicha investigación es estandarizar la política y adecuarla a la buena práctica seleccionada.

3.1.1.2 Defensa contra software malicioso

Para la realización del análisis financiero asociado a esta política, es necesario reconocer que esta política forma parte de la propuesta realizada pero no cuenta con desarrollo de procesos *As-Is* debido a que no forma parte del quehacer cotidiano de la empresa. Además, al tratarse de procesos nuevos, no pueden ser sujetos a simulaciones.

Por tanto, para el cálculo de la métrica *ROI,* se deben tomar en cuenta la siguiente información:

- En cuanto a la ganancia, una de las principales dificultades de no contar con herramientas antivirus es el riesgo relacionado al robo o desaparición de información, sobre esto, Statista (2017) menciona que para el año 2020 un 35% de la información almacenada en los repositorios organizacionales requiere de medidas de seguridad, pero se encuentra

desprotegida. Siendo así, en el **¡Error! No se encuentra el origen de la referencia.** se d etermina que el costo total de las laptops, que son los principales repositorios de información de la organización, es de ₡20.000.000, por tanto, el cálculo a realizar sería el siguiente:

₡20.000.000 * 0.35 = ₡7.000.000

Por tanto, según las estadísticas aportadas, los mencionados ₡7.000.000 corresponden a la ganancia obtenida de implementar esta política.

- Respecto al costo total de la inversión para esta política, es necesario tomar en cuenta las dieciséis semanas en las que el investigador desarrolló la propuesta. Según se muestra en la Tabla 5. Salario investigador, el costo relacionado con el investigador, de forma semanal, es de ¢223.119,105 y la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado con lo anteriormente mencionado sería el siguiente:

¢223.119,105 * 16 = ¢3.569.905,68

Por tanto, el costo total de la inversión es de ¢3.569.905,68.

En conclusión, y tomando en cuenta las premisas detalladas sobre ganancia e inversión, y basándose en la Ilustración 17. Fórmula ROI, el cálculo de la métrica *ROI* se realiza según lo indicado en la Ilustración 19. Cálculo ROI Defensa contra software malicioso.

Ilustración 19. Cálculo ROI Defensa contra software malicioso

$$\frac{₡7.000.000 - ¢3.569.905,68}{¢3.569.905,68} = 0,96$$

Fuente: Elaboración propia, 2022.

Según lo mostrado en la Ilustración 19. Cálculo ROI Defensa contra software malicioso se determina que el retorno de la inversión es el resultante del cálculo:

0,96 * 100 = 96%

Lo que se puede traducir a un retorno de la inversión alto. Sin embargo, se debe recordar que el desarrollo de esta propuesta está enfocado en el uso y estandarización de las políticas de seguridad en la organización, por lo que, de momento, no está en el alcance del proyecto proyectar retornos de inversión altos producto de la aplicación de las políticas. Por tanto, se concluye que el *ROI* no es una métrica determinante para el éxito de la propuesta.

3.1.1.3 Inventario y control de los activos de software

Para la realización del análisis financiero de esta política, se debe tomar en cuenta que, esta política es nueva en la organización, por tanto, sus procesos no pueden ser sometidos a simulaciones.

Por tanto, para el cálculo de la métrica *ROI,* se deben tomar en cuenta las premisas detalladas a continuación:

- Para determinar la ganancia, es necesario conocer que una de las principales desventajas de no ejecutar procesos relacionados al inventariado de los activos de software es la pérdida que se pueda dar de los mismos. Para esto, Seareach (2018) menciona que las computadoras tipo laptops son uno de los activos más propensos a extraviarse, brindando un porcentaje de 14% de probabilidad de extravío sobre el total de equipos laptops. Siendo así, se determinó que la organización cuenta con un total de cuarenta laptops, por tanto, el 14% de ese total corresponde a 5.6, lo que para efectos prácticos se tomará como un total de cinco laptos. Además, se menciona que cada equipo está valorado en ₡500.000, por tanto, el monto total de laptops propensas a extraviarse se calcula de la siguiente manera:

  ₡500.000 * 5 = ₡2.500.000

  Además, Seareach (2018) comenta que cuando un activo se extravía es común pensar que basta únicamente con reponer el activo, sin embargo, la pérdida de una laptop conlleva a actividades y pérdida de información que tienen un costo adicional asociado. Este costo es determinado en un total de £249 (doscientos cuarenta y nueve libras esterlinas) por

equipo, lo cual se traduce a ₡186.592,00 por equipo. Para el total de laptops propensas a extraviarse el cálculo sería de la siguiente manera:

₡186.592,00 * 5 = ₡932.960

Dados los anteriores cálculos, en la Tabla 8. Ganancia total Inventario y control de activos de software se muestra el resumen y suma total de la ganancia esperada, teniendo como total la suma de ₡3.435.960. Cabe destacar que estas estadísticas son tomadas como ganancia ya que es el ahorro que tendría la organización si implementa la política y procesos propuestos.

Tabla 8. Ganancia total Inventario y control de activos de software

Estadística	Costo
Costo total de laptops propensas a extraviarse	₡2.500.000
Costos asociados al extravío de las laptops	₡932.960
Total	₡3.435.960

Fuente: Elaboración propia, 2022.

- Respecto a la inversión para esta política, es necesario tomar en cuenta las dieciséis semanas con las que contó el investigador para el desarrollo de la propuesta. Según se muestra en la Tabla 5. Salario investigador el costo relacionado al investigador de forma semanal es de ¢223.119,105 y la investigación abarcó un total de dieciséis semanas. Por tanto, el cálculo relacionado a lo anteriormente mencionado sería el siguiente:

  ¢223.119,105 * 16 = ¢3.569.905,68

  Por tanto, el costo total de la inversión es de ¢3.569.905,68.

Tomando en cuenta las anteriores premisas y basado en la Ilustración 17. Fórmula ROI el cálculo para determinar la métrica *ROI* sería el que se evidencia en la Ilustración 20. Cálculo ROI Inventario y control de los activos de software.

Ilustración 20. Cálculo ROI Inventario y control de los activos de software

$$\frac{₡3.435.960 - ¢3.569.905,68}{¢3.569.905,68} = -0,03$$

Fuente: Elaboración propia, 2022.

Según lo mostrado en la Ilustración 20. Cálculo ROI Inventario y control de los activos de software se determina que el retorno de la inversión es el resultante del cálculo:

-0,3 * 100 = -30%

Lo que se puede traducir a un retorno de la inversión negativo que implica una inversión mayor a lo percibido como ganancia. Sin embargo, cabe destacar que esta métrica arroja el retorno de la inversión sobre la situación actual, lo que quiere decir que si la organización sigue en crecimiento el retorno de la inversión crecerá. Además, se debe recordar que el desarrollo de esta propuesta está enfocado en la orientación de las políticas de seguridad hacia las buenas prácticas, y en estandarizas su uso sobre la totalidad de tribus de la organización, por tanto, el retorno de la inversión no es un indicador clave para el éxito de esta propuesta.

Bibliografía

Seareach. (2018). Lost or Stolen Assets Cost Businesses Mora than Just Replacement Items. https://www.seareach.co.uk/blog/lost-or-stolen-assets-cost-more/

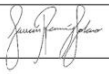
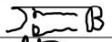
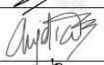
Statista. (2017). Actual status of data security worldwide from 2010 to 2025. https://www.statista.com/statistics/815167/worldwide-actual-status-of-data-security/

Apéndice N - Minuta EM 07 – 2008

Minuta de reunión 07

XUM TECH
EXPERIENCIA DIGITAL

Fecha:	20/08/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Si	
Dayana Vindas	Si	
Andrea Alpízar	Si	
Jose Ramirez	Si	
Sussana Ramirez	Si	
Josué Solís	Si	
Mauricio Cascante	Si	
Zimri Zamora	Si	
Selenia Orozco	Si	
Anjelica Tristani	Si	
Maribel Cordero	Si	

Temas tratados	
No.	**Tema**
1	Grupo focal para determinar tiempos de las actividades de la política de control y uso de privilegios administrativos.

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	**Firma de minuta**	**Sergio Arroyo**	

Notas:

Se realiza un grupo focal, mediante una video llamada, en la que se consulta a los participantes los tiempos máximos y mínimos involucrados en cada actividad de la política sobre Control y uso de privilegios administrativos, la cual actualmente conocen como Uso de Keepass. Se hizo un repaso por todos los procesos empleados para la política, y de cada proceso se determinó un tiempo mínimo y un tiempo máximo, obteniendo la siguiente información:

Proceso:	Configuración Inicial	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Descargar la herramienta Keepass	1	5
Instalar la herramienta Keepass	2	3
Ingresar a herramienta Keepass	0,25	1
Buscar y seleccionar base de datos de credenciales	10	15
Solicitar clave de acceso a credenciales	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a "Credenciales.kdbx"	0,5	1

Proceso:	Crear Usuario	
Actividad	Duración mínima en minutos	Duración máxima en minutos

Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Ubicar la sección en la que se desea crear el usuario	1	2
Ingresar nombre de usuario	1	3
Ingresar contraseña	1	3
Ingresar enlace del ambiente	1	3
Guardar el usuario	0,25	1
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

Proceso:	Actualización de usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60

Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Actualizar el usuario deseado	1	2
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

Proceso:	Consulta de usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2

Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Consultar el usuario deseado	2	5

Proceso:	Eliminar usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Eliminar el usuario deseado	2	5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

Minuta de reunión 08

Fecha:	23/08/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	**Si**	
Alex Ureña	**Si**	

Temas tratados	
No.	**Tema**
1	**Definición de tiempos para nuevas actividades de política de Control y Uso de privilegios administrativos.**

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	**Firma de minuta**	**Sergio Arroyo**	

Notas:

Se realiza una sesión con Alex Ureña en la cual se le presentan los procesos To-Be. Una vez aprobados, se le consulta sobre los tiempos asociados a las actividades de los procesos de la política de control y uso de privilegios administrativos, ya que es necesario definir tiempos asociados a aquellos que presentaron cambios, según el análisis de la brecha realizado en este proyecto. Por tanto, se brindan las siguientes definiciones:

- Para el proceso denominado “Configuración inicial”, según la revisión de la brecha se determinó que este no tuvo cambios conforme a su versión As-Is; se toma la decisión de mantener los tiempos tal cual fueron definidos en el grupo focal.

Proceso:	Configuración Inicial	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Descargar la herramienta Keepass	1	5
Instalar la herramienta Keepass	2	3
Ingresar a herramienta Keepass	0,25	1
Buscar y seleccionar base de datos de credenciales	10	15
Solicitar clave de acceso a credenciales	20	60
Solicitar clave a líder de tribu	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a "Credenciales.kdbx"	0,5	1

- Para el proceso llamado “Consulta de usuarios”, se realizó la revisión de la brecha y se determinó que este no tuvo cambios conforme a su versión As-Is, por tanto, se toma la decisión de mantener los tiempos tal cual fueron definidos en el grupo focal.

Proceso:	Consulta de usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60

Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Consultar el usuario deseado	2	5

- Para el proceso que lleva como nombre “Eliminar usuarios”, se realizó la revisión de la brecha y se identificó que existen actividades nuevas, para las cuales se determina lo siguiente:
    - Informar sobre el requerimiento de borrado del usuario: La tarea consiste en informar al líder de tribu sobre el requerimiento de borrar un usuario de la herramienta Keepass. Para esta tarea, se considera un tiempo mínimo de 2 minutos y un máximo de 5.
    - Analizar requerimiento de borrado del usuario: Consiste en que el líder de la tribu analiza si el usuario por eliminar debe o no serlo. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.
    - Brindar respuesta al colaborador: El líder de la tribu da respuesta al colaborador sobre si se debe eliminar o no el usuario. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.

Proceso:	Eliminar usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Informar sobre el requerimiento de borrado del usuario	2	5

Analizar requerimiento de borrado del usuario	2	5
Brindar respuesta al colaborador	2	5
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Eliminar el usuario deseado	2	5
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

- Para el proceso denominado “Actualización de usuarios”, se revisa la brecha identificada y se identifica que existen actividades nuevas, para las cuales se decide lo siguiente:
    - Informar sobre el requerimiento de borrado del usuario: La tarea consiste en informar al líder de tribu sobre el requerimiento de borrar un usuario de

la herramienta Keepass. Para esta tarea se considera un tiempo mínimo de 2 minutos y uno máximo de 5.

- Analizar requerimiento de borrado del usuario: Consiste en que el líder de la tribu analiza si el usuario por eliminar debe o no ser eliminado. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.
- Brindar respuesta al colaborador: El líder de la tribu da respuesta al colaborador sobre si se debe eliminar o no el usuario. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.

Proceso:	Actualización de usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Informar sobre el requerimiento de borrado del usuario	2	5
Analizar requerimiento de borrado del usuario	2	5
Brindar respuesta al colaborador	2	5
Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1

Sincronizar herramienta keepass	0,5	1
Actualizar el usuario deseado	1	2
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

- Para el proceso llamado “Crear usuario”, se revisa la brecha identificada y se observa que existen actividades nuevas, para las cuales se decide lo siguiente:
    - Informar sobre el requerimiento de borrado del usuario: La tarea consiste en informar al líder de tribu sobre el requerimiento de borrar un usuario de la herramienta Keepass. Se considera un tiempo mínimo de 2 minutos y uno máximo de 5.
    - Analizar requerimiento de borrado del usuario: Consiste en que el líder de la tribu analiza si el usuario por eliminar debe o no ser eliminado. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.
    - Brindar respuesta al colaborador: El líder de la tribu da respuesta al colaborador sobre si se debe eliminar o no el usuario. Se considera que esta tarea tiene un mínimo de 2 minutos y un máximo de 5.
    - Examinar si el usuario por crear ya existe: El colaborador revisa la herramienta Keepass con el fin de determinar si el usuario por crear ya existe. Se considera un tiempo mínimo de 1 minuto y uno máximo de 2.

Proceso:	Crear Usuario	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Informar sobre el requerimiento de borrado del usuario	2	5
Analizar requerimiento de borrado del usuario	2	5
Brindar respuesta al colaborador	2	5

Ingresar a herramienta Keepass	0,25	1
Solicitar clave de acceso a líder de tribu	20	60
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Brindar clave de acceso a credenciales	1	2
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Examinar si el usuario a crear ya existe	1	2
Ubicar la sección en la que se desea crear el usuario	1	2
Ingresar detalles del nuevo usuario	1	3
Guardar el usuario	0,25	1
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1

- Para el proceso “Revisión de usuarios”, se identifica que, a pesar de ser un proceso nuevo, muchas de las actividades ya cuentan con tiempo obtenido del grupo focal, por tanto, se define lo siguiente para cada actividad:

Proceso:	Revisión de usuarios	
Actividad	Duración mínima en minutos	Duración máxima en minutos
Ingresar a la herramienta Keepass	0,25	1

Brindar clave de acceso a credenciales	1	2
Solicitar clave a dueño de producto	20	60
Brindar clave de acceso a credenciales	1	2
Revisión de los usuarios registrados	20	60
Solicitar clave de acceso a Líder de tribu	20	60
Ingresar clave de acceso a credenciales	0,5	1
Sincronizar herramienta keepass	0,5	1
Guardar los cambios efectuados en "Credenciales.kdbx"	0,5	1
Eliminar Usuarios	20	60
Actualizar Usuarios	20	60

Apéndice P - Minuta EM 09 – 2508

Minuta de reunión 09

Fecha:	25/08/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Sergio Arroyo Torres	Sí	
Alex Ureña	Sí	

Temas tratados	
No.	**Tema**
1	Definición de monto total en inventario de laptops

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
1	Firma de minuta	Sergio Arroyo	

Notas:

Se realiza una sesión con Alex Ureña en la cual se le expresa la necesidad que se tiene en la investigación de contar con el monto total en laptops de la organización. Se le hace saber que este monto es necesario para realizar cálculos en el análisis financiero de las políticas propuestas. Ante la consulta, el entrevistado procede a revisar documentos contables, lo cual le permite asegurar que el monto en laptops asciende a ₡20.000.000 para un total de 40 laptops; esto determina que cada equipo está valorado en ₡500.000.

Apéndice Q - Minuta RV 04 – 2208

Revisión documental 04

No. Revisión	**04**
Fecha:	**22/08/2022**
Responsable	**Sergio Arroyo Torres**

Detalles del cambio	
Motivo de la revisión	Determinar la estrategia a tomar para la simulación de los procesos pertenecientes a las políticas de seguridad no existentes en la organización (sin escenario As-is)
Fuente consultada	**Sitio web:** Towards Data Science **Artículo:** Using Simulation Studies to Motivate Modelling Decisions **Enlace:** https://towardsdatascience.com/using-simulation-studies-to-motivate-modelling-decisions-be8bae2cd1c2

Hallazgos	
No.	**Impacto**
01	Los estudios de simulación son de interés cuando hay una falta de orientación en la literatura o cuando los métodos son novedosos.

Aprobación	
Estado	**Motivo**
Aprobado / Rechazado	**Aprobado**

Revisión documental 05

No. Revisión	**05**
Fecha:	**23/08/2022**
Responsable	**Sergio Arroyo Torres**

Detalles del cambio	
Motivo de la revisión	Determinar la estrategia a tomar para la realización del análisis financiero para la política “Defensa contra software malicioso”
Fuente consultada	**Sitio web:** Statista **Artículo:** Actual status of data security worldwide from 2010 to 2015 **Enlace:** https://www.statista.com/statistics/815167/worldwide-actual-status-of-data-security/

Hallazgos	
No.	**Impacto**
01	Para el año 2020, el 35% de la información que requiere ser protegida, no se encuentra protegida. Por tanto, como los principales repositorios de información de la organización son las laptops de cada colaborador, el costo de no proteger los equipos será calculado sobre el costo total de los equipos.

Aprobación

Estado	Motivo
Aprobado / Rechazado	**Aprobado**

Revisión documental 06

No. Revisión	**06**
Fecha:	**24/08/2022**
Responsable	**Sergio Arroyo Torres**

Detalles del cambio	
Motivo de la revisión	Determinar la estrategia a tomar para la realización del análisis financiero para la política “Inventario y control de los activos de software”
Fuente consultada	**Sitio web:** Seareach **Artículo:** Lost or stolen assets cost businesses mora than a just replacement items **Enlace:** https://www.seareach.co.uk/blog/lost-or-stolen-assets-cost-more/

Hallazgos	
No.	**Impacto**
01	14% de los activos extraviados pertenecientes a los colaboradores son laptops.
02	Además del costo relacionado al reemplazo del activo, para las laptops se debe tomar en cuenta un costo adicional de 249 libras esterlinas por equipo.

Aprobación	
Estado	**Motivo**

Aprobado / Rechazado	**Aprobado**

Apéndice T – Minuta AC 01- 2202

Minuta de reunión académica 01

XUM TECH
EXPERIENCIA DIGITAL

Fecha:	22/02/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Cronograma.
02	Objetivos
03	Programación de sesión con contraparte

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Actualizar cronograma	Sergio Arroyo	01/03/2022
02	Actualización de objetivos	Sergio Arroyo	01/03/2022

Notas:

Se revisa el cronograma de proyecto. Se evidencias fallas que serán corregidas y mostradas en la próxima sesión. Se revisan los objetivos y se propone corregirlo para la próxima sesión. Además, se acuerda programar la primera sesión con la contraparte.

Apéndice U – Minuta AC 02- 2302

Minuta de reunión académica 02

Fecha:	23/02/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	
Alex Ureña	Si	

Temas tratados	
No.	**Tema**
01	Presentación de la profesora tutora
02	Acuerdos y obligaciones de la contraparte
03	Metodología de trabajo

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Programación de siguiente sesión con contraparte	Sergio Arroyo	05/03/2022

Notas:

La profesora tutora Yarima Sandoval se presenta a Alex Ureña como la profesora a cargo del TFG de Sergio Arroyo. La profesora explica a la contraparte las obligaciones de la organización, la metodología de trabajo y las próximas sesiones.

Apéndice V - Minuta AC 03- 0103

Minuta de reunión académica 03

Fecha:	01/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Revisión de Cronograma.
02	Revisión de Objetivos
03	Entrega de capítulo 1

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Subir cronograma	Sergio Arroyo	05/03/2022
02	Cargar Capítulo 1	Sergio Arroyo	05/03/2022
03	Presentación de primera versión de encuesta	Sergio Arroyo	08/03/2022

Notas:

En esta sesión, se realiza la revisión sobre los objetivos y cronograma del proyecto. Quedan como tareas pendientes la presentación de la primera versión de la encuesta a realizar. Además, se indica al estudiante que debe cargar en la plataforma el cronograma relacionado. Y para finalizar, se realizan las primeras correcciones sobre la encuesta a aplicar a la organización.

Apéndice W - Minuta AC 04- 1103

Minuta de reunión académica 04

Fecha:	11/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Revisión de primera versión de encuesta
02	Revisión de Objetivos
03	Correcciones a capítulo 1

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Presentación de segunda versión de encuesta	Sergio Arroyo	
02	Presentación de correcciones a capitulo 1	Sergio Arroyo	
03	Presentación de objetivos corregidos	Sergio Arroyo	

Notas:

En esta sesión, se realiza la revisión sobre los objetivos a lo que se establece una versión final. Se recomienda revisarlos más adelante, para identificar si requieren un cambio. Se conversa sobre el marco de referencia del TFG, el cual se seleccionó con Alex Ureña. Se selecciona COBIT 5 como marco de referencia.

Apéndice X - Minuta AC 05- 1403

Minuta de reunión académica 05

Fecha:	14/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Explicación sobre metodología alternativa a cargo del Sr. Luis Naranjo

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Tomar decisión sobre si usar o no la metodología alternativa.	Sergio Arroyo	

Notas:

Se realiza una sesión con el señor Luis Naranjo en la cual explica como llevar a cabo un proyecto bajo la metodología alternativa. Producto de esta sesión el estudiante debe analizar si su proyecto puede ser implementado bajo dicha metodología.

Apéndice Y - Minuta AC 06- 1503

Minuta de reunión académica 06

Fecha:	15/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Metodología alternativa
02	Revisión de segunda propuesta de encuesta
03	Correcciones capítulo 1

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Inicio del capítulo 2		
02			
03			

Notas:

Se conversa con la profesora tutor sobre la metodología alternativa, y se le da el visto bueno para que el proyecto se realice mediante esta metodología. La profesora propone que, al avanzar esta metodología, sea sometida a revisión por parte del señor Luis Naranjo con el fin de contar con el feedback adecuado.

Se revisa la segunda versión de la encuesta, siendo aprobada según recomendaciones de la profesora tutora.

Se muestra a la profesora las correcciones del capítulo 1, siendo aprobados por la tutora.

Apéndice Z - Minuta AC 07- 2503

Minuta de reunión académica 07

Fecha:	25/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Revisión de avance sobre segundo capítulo: conceptual

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Continuar construyendo el capítulo 2	Sergio Arroyo Torres	
02			
03			

Notas:

Se revisa el avance sobre el capítulo 2, a lo que la profesora tutora indica que el avance es más lento de lo esperado. Además, la profesora recomienda incluir los controles CIS.

Apéndice AA - Minuta AC 08- 3003

Minuta de reunión académica 08

Fecha:	30/03/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Avance Capítulo 2
02	Avance capítulo 3

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Avances relacionados a los rubros de la dimensión axiológica.	Sergio Arroyo	

Notas:

Se muestra el avance del capítulo 2, a lo que la tutora responde que de momento se visualiza bien, pero, que más adelante según el avance se debe revisar para corroborar que no se deba agregar más conceptos. En cuanto al capítulo 03, se mencionan dudas como las relacionadas a los instrumentos de investigación, ya que se desconoce por parte del estudiante si al tratarse de metodología alternativa se deben incluir los instrumentos, a lo que la tutora responde que sí.

Apéndice AB - Minuta AC 09- 0504

Minuta de reunión académica 09

Fecha:	05/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Rubros para medición de la dimensión axiológica en el capítulo 3

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Corrección sobre los rubros de medición de la dimensión axiológica	SergioArroyo	
02			
03			

Notas:

Se revisan los rubros definidos para la medición de las oportunidades de mejora y de la efectividad. La tutora realiza recomendaciones sobre estas que el estudiante deberá realizar.

Apéndice AC - Minuta AC 10- 0604

Minuta de reunión académica 10

Fecha:	06/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	
Alex Ureña	Si	

Temas tratados	
No.	**Tema**
01	Avance del proyecto
02	Nivel de satisfacción
03	Tiempo de ejecución

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Comunicar avance a Alex Ureña		
02			
03			

Notas:

Se realiza la segunda sesión de seguimiento del proyecto con la contraparte de la empresa en la cual se le consulta sobre el avance del proyecto y el nivel de satisfacción. Alex indica que el estudiante se esta desempeñando de buena manera. Además, la tutora explica sobre las necesidades del estudiante en cuanto a tiempo para el TFG.

Apéndice AD - Minuta AC 11- 2104

Minuta de reunión académica 11

Fecha:	21/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Rubros para medición de la dimensión axiológica
02	Consultas sobre fases de ejecución

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Corrección de las fases del proyecto	Sergio Arroyo	
02	Aplicar correcciones sobre los rubros de medición	Sergio Arroyo	

Notas:

En esta sesión, se muestran los rubros de medición de la dimensión axiológica ya corregidos según las observaciones de las anteriores sesiones. Además, el estudiante consulta sobre el funcionamiento de las fases de ejecución, ya que no tiene muy clara su implementación. Al recibir retroalimentación, queda como compromiso para la próxima sesión mostrar el avance.

Apéndice AE - Minuta AC 12- 2604

Minuta de reunión académica 12

Fecha:	26/04/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Fases de ejecución del proyecto
02	Matriz de trazabilidad

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Correcciones matriz de trazabilidad	Sergio Arroyo	

Notas:

En esta sesión, se muestran las fases del proyecto ya corregidas, a lo que la tutora responde de forma positiva. Además, según este avance, se muestra la primera versión de la matriz de trazabilidad. A esta la tutora realiza correcciones.

Apéndice AF - Minuta AC 13- 0505

Minuta de reunión académica 13

Fecha:	05/05/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Matriz de trazabilidad
02	Revisión del análisis de los resultados de la encuesta

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Corrección de gráficos del análisis de la encuesta	Sergio Arroyo	

Notas:

En esta sesión, se da visto bueno a la matriz de trazabilidad corregida, además, se muestra a la profesora tutora una propuesta sobre el análisis realizado sobre los resultados de la encuesta. La profesora accede al análisis, sin embargo, pide corregir los gráficos para que lleven la frase “Elaboración propia, 2022”.

Apéndice AG - Minuta AC 14- 0605

Minuta de reunión académica 14

Fecha:	06/05/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	
Alex Ureña	Si	

Temas tratados	
No.	**Tema**
01	Extensión del tiempo para el desarrollo del TFG
02	Expectativas de la empresa
03	

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Llenado de solicitud para IN	Sergio Arroyo	

Notas:

En esta sesión, se discute con la tutora y la contraparte de la empresa la posibilidad de llenar la boleta de IN, lo que brinda la posibilidad de la extensión del proceso de realización del TFG, esto por problemas de tiempos asociados al tiempo de trabajo. Tanto la tutora como la contraparte de la empresa acceden a dicha solicitud.

Apéndice AH - Minuta AC 15- 1205

Minuta de reunión académica 15

Fecha:	12/05/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Avances capítulo 4

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01		Sergio Arroyo	
02		Sergio Arroyo	
03		Sergio Arroyo	

Notas:

Para el cumplimiento del IN, es necesario que el estudiante tenga finalizado el capítulo 4, correspondiente al Análisis de resultados. Siendo así, en esta sesión se abarcan temas relacionados a consultas respecto a la diagramación As-is, ya que la propuesta abarca la políticas nuevas que no cuentan con documentación necesaria para realizar la diagramación As-is, por tanto, se decide en conjunto que, con la base debida, estas políticas no cuentan con diagramación As-is.

Apéndice AI - Minuta AC 16- 2505

Minuta de reunión académica 16

Fecha:	25/05/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Presentación de medición de oportunidades de mejora
02	Revisión de diagramación As-is

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Culminar capítulo 4	Sergio Arroyo	

Notas:

En esta sesión, se muestra el avance respecto a la diagramación As-is según los acuerdos realizados. Además de esto, se muestra la medición sobre la oportunidad de mejora de los procesos realizada según los rubros definidos en la axiología. Además, se repasan los puntos pendientes para la finalización del capítulo.

Apéndice AJ - Minuta AC 17- 3005

Minuta de reunión académica 17

XUM TECH
EXPERIENCIA DIGITAL

Fecha:	30/05/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Revisión general de capítulo 4

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Culminación de capítulo 4	Sergio Arroyo	

Notas:

En esta sesión, se realiza la revisión del capítulo 4 finalizado, esto para poder ingresar al tiempo de IN según la solicitud firmada.

Apéndice AK - Minuta AC 18- 1409

Minuta de reunión académica 18

Fecha:	15/09/2022

Asistencia		
Nombre	**Asistencia**	**Firma de conformidad**
Yarima Sandoval	Si	
Sergio Arroyo	Si	

Temas tratados	
No.	**Tema**
01	Revisión general de TFG

Tareas por realizar			
No.	**Tarea**	**Responsable**	**Fecha de entrega**
01	Agregar sección "Construcción de la propuesta"	Sergio Arroyo	
02	Revisar salarios	Sergio Arroyo	

Notas:

En esta sesión, se realiza la revisión general sobre el TFG realizado durante el periodo de IN. Sobre este, la tutora encuentra dos puntos a revisar. El primero, recomienda agregar una sección llamada "Construcción de la propuesta" la cual se debe incluir sobre el capítulo cuatro y debe hacer énfasis a las estrategias que se llevarán a cabo en la propuesta de solución. Además, recomienda revisar los montos utilizados para salarios, para que estos incluyan las garantías sociales.

Apéndice AL – Firma minutas empresariales

NOTA ACLARATORIA Aprobación de minutas TFG

Ante la situación que enfrenta el país por la pandemia mundial, se aprueban por parte del Sr. Alex Ureña Cordero, las siguientes minutas correspondientes al proyecto de graduación: Propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech. Realizado por el estudiante Sergio Arroyo Torres, carné 2013087502, cédula 304840546.

A continuación, se muestra la lista de las minutas aprobadas por el Sr. Alex Ureña:

- Minuta AC 02- 2302
- Minuta AC 10- 0604
- Minuta AC 14- 0605
- Minuta EM 02 – 0504
- Minuta EM 06 – 1706
- Minuta EM 08 – 2308
- Minuta EM 09 – 2508

ALEX UREÑA CORDERO (FIRMA)

Digitally signed by ALEX UREÑA CORDERO (FIRMA)
Date: 2022.09.19 22:40:12 +02'00'

Sr. Alex Ureña Cordero

Apéndice AM – Firma minutas académicas

NOTA ACLARATORIA Aprobación de minutas TFG

Ante la situación que enfrenta el país por la pandemia mundial, se aprueban por parte de la Ing. Yarima Sandoval Sánchez, M.A.E, las siguientes minutas correspondientes al proyecto de graduación: Propuesta de políticas de seguridad de la información mediante la utilización de buenas prácticas de la industria para la empresa Xumtech. Realizado por el estudiante Sergio Arroyo Torres, carné 2013087502, cédula 304840546.

A continuación, se muestra la lista de las minutas aprobadas por la Ing. Yarima Sandoval Sánchez, M.A.E:

- Minuta AC 01- 2202
- Minuta AC 02- 2302
- Minuta AC 03- 0103
- Minuta AC 04- 1103
- Minuta AC 05- 1403
- Minuta AC 06- 1503
- Minuta AC 07- 2503
- Minuta AC 08- 3003
- Minuta AC 09- 0504
- Minuta AC 10- 0604
- Minuta AC 11- 2104
- Minuta AC 12- 2604
- Minuta AC 13- 0505
- Minuta AC 14- 0605
- Minuta AC 15- 1205
- Minuta AC 16- 2505
- Minuta AC 17- 3005
- Minuta AC 18- 1509

Ing. Yarima Sandoval Sánchez, M.A.E