FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍAS

Tesis

Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa Replica S.R.L. 2019

Para optar el título profesional de Ingeniero de Sistemas e Informática

AUTORA

Br. Rupay Velazco, Merlin Stefanny

LÍNEA DE INVESTIGACIÓN DE LA UNIVERSIDAD

Ingenierías de Sistemas e Informática, Industrial y Gestión Empresarial y Ambiental

LIMA - PERÚ

2019

“Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa Replica S.R.L. 2019”

Miembros del Jurado

Presidente del Jurado

Mg. Walter Amador Chávez Alvarado

Secretario

Dr. Davis Rivera Gómez

Vocal

Mtro. Nicolas Fedeberto Ortiz Vargas

Asesor metodólogo

Mg. Fernando Alexis Nolazco Labajos

Asesor temático

Mg. Luis Enrique Ramirez Pacheco

Dedicatoria

Este trabajo va dedicado a mis padres Rupay Limache, Elmer White y Velazco Valenzuela, Patricia Margarita, quienes me brindaron el apoyo necesario para no dejar de esforzarme y alcanzar mis objetivos y metas sembradas a lo largo de mi existencia. Ustedes son y serán siempre el motivo por el cual buscaré constantemente la superación personal.

Por último, el agradecimiento a mis tíos Velasco Quispe, Mery y a mi abuelo Velazco Aguilar, Manuel Gustavo que siempre me inculcaron los valores para continuar sin obstáculos.

Agradecimiento

Agradecer a Dios por el don de la vida y las diversas oportunidades que me ha brindado para hacer realidad este proyecto. Agradezco a la Universidad Norbert Wiener, por darme la oportunidad de estudiar y llegar a ser el profesional que soy hoy en día.

También los directivos y compañeros de la empresa Replica S.R.L., por darme la oportunidad de formar parte de su equipo de trabajo del área tecnológica de Proyectos - ATP, y apoyarme con mi desarrollo y desenvolvimiento personal.

Declaración de autenticidad y responsabilidad

Yo, Rupay Velazco Merlin Stefanny identificada con DNI Nro 73023429, domiciliado en AA.HH. Daniel Alcides Carrión Mz. N Lote 20 – San Martin de Porres egresada de la carrera profesional de Ingeniería de Sistemas e Informática he realizado la Tesis titulada "Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa Replica S.R.L. 2019" para optar el título profesional de Ingeniero, para lo cual Declaro bajo juramento que:

1. El título de la Tesis ha sido creado por mi persona y no existe otro trabajo de investigación con igual denominación.
2. En la redacción del trabajo se ha considerado las citas y referencias con los respectivos autores y no existe copia o plagio alguno.
3. Después de la revisión de la tesis con el software Turnitín se declara 14% de coincidencias.
4. Para la recopilación de datos se ha solicitado la autorización respectiva a la empresa u organización, evidenciándose que la información presentada es real.
5. La propuesta presentada es original y propia del investigador no existiendo copia alguna.
6. En el caso de omisión, copia, plagio u otro hecho que perjudique a uno o varios autores es responsabilidad única de mi persona como investigador eximiendo de todo a la Universidad Privada Norbert Wiener y me someto a los procesos pertinentes originados por mi persona.

Firmado en Lima el día 15 de agosto del 2019.

Rupay Velazco Merlin Stefanny

DNI 73023429

Presentación

La presente tesis titulada “Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa Replica S.R.L. 2019”, se desarrolló con el objetivo de reducir la perdida de información de la empresa y mejorar las políticas de seguridad, se utilizó las herramientas del portal de administrador de Office 365, para analizar, configurar y mejorar los accesos de los usuarios, el control de los archivos por áreas y permisos respectivos, la propuesta la alineamos a la visión de la empresa. El estudio fue beneficioso para cumplir con el reglamento de Grados y Títulos de la universidad Privada Norbert Wiener, con el propósito de optar al Título de Ingeniero de Sistemas e Informática.

El estudio se encuentra estructurado por ocho capítulos, el cual se ha empleado hasta el capítulo cinco para el análisis del problema y llegar al capítulo seis para proponer la solución óptima para la empresa, a continuación, se detalla cada capítulo desarrollado:

Capítulo I está compuesto por el problema de investigación en el cual se describirá el problema de la empresa en estudio y la formulación del problema que se desarrollará y dará solución, planteando los sucesos internacionales, nacionales y empresariales, también consta de los objetivos generales y específicos que son muy importantes clasificar que ayudarán a la investigación, se encuentra la justificación metodológica y practica que para la ejecución del problema se usó la exploración holística proyectiva. Capítulo II contiene sustento teórico para complementar a la categoría solución, las teorías donde nos apoyamos en las distintas teorías que existe para sustentar el problema y la solución de la investigación, se basa en los antecedentes nacionales e internacionales que consta de tesis, artículos o libros que dan sustento a la investigación que estamos realizando. Capítulo III se muestra el método inductivo y deductivo que apoya al estudio , donde se da a conocer que se basa en un enfoque mixto ya que se usan tanto lo cuantitativo y lo cualitativo, dando un panorama de diferentes perspectivas también se desarrolla de cuanto consta la población y que unidades informantes intervienen y cuáles son los análisis de datos que comprende para nuestra muestra obtenida por conveniencia se aplicó un registro de datos y entrevista para la recopilación de datos; Capítulo IV interviene toda trabajo que se realizó en la empresa, las entrevistas, los registros

de datos, los resultados cuantitativos y cualitativos de cada uno de ellos; Capítulo V se basa en el desarrollo de lo que implica la propuesta se describe y detallada la elección de alternativas para solucionar el problema, se presentan qué objetivos se tomaran para apoyar a la solución, y que resultados esperamos sobre esta propuesta; Capítulo VIII hace referencia a las conclusiones y sugerencias basándose en el objetivo general y especifico, por último el Capítulo IX que se refiere a las referencias, fuentes de conocimiento, imágenes, matrices obtenidas de toda la investigación.

Autora: Rupay Velazco, Merlin Stefanny
DNI: 73023429

Índice

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

La siguiente investigación con título “Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa comercial - 2019”, tuvo como objetivo aumentar la Protección de la información que utilizan con frecuencia los trabajadores de la empresa dentro de la plataforma de office 365 segmentando documentos de data sensible y mejorando la seguridad de los accesos a sus cuentas de correo.

Dentro del estudio se utilizó el sintagma holístico, mediante un enfoque mixto y de tipo proyectiva, donde se aplicaron los métodos de recolección cuantitativa y cualitativa, con el propósito de establecer la realidad problemática dentro de la empresa. Para ello se entrevistó a tres usuarios con los cargos respectivos de director, gerente y jefe del área, así mismo se extrajeron registros de auditoria con los accesos de los usuarios desde ambientes externos e internos, los usuarios que manejan información referente a la empresa y que servicio utilizan más si SharePoint o OneDrive, ya que desde estos servicios se acceden a documentos y pueden ser eliminados y o descargados; así mismo estas herramientas estaban directamente relacionadas con el marco teórico descrito dentro de la investigación.

En conclusión, luego de realizar el trabajo de campo y elaborar una triangulación entre los datos recolectados de manera cuantitativa y cualitativamente, se logró diagnosticar que se tienen políticas básicas aplicadas a los usuarios de la empresa, identificando el problema solución que permitió formular una propuesta de investigación basado en la aplicación de políticas de seguridad en dispositivos móviles, autenticación por usuario, mejorar el control de acceso a los datos mapeándolos por áreas, capacitar a los usuarios en el uso de sus cuentas y dispositivos que tienen acceso a la información y la documentación de las mismas con la finalidad de mejorar las políticas y el control de la plataforma y los archivos de data sensible que pertenece a la empresa.

Palabras clave: Protección de la información, políticas de seguridad, plataforma Cloud office 365.

Abstract

The following research entitled "Implementing policies to reduce the risk of information loss on the Cloud office 365 platform in the trading company - 2019", aimed to increase the protection of frequently used information Replica workers within the 365 office platform by segmenting sensitive data documents and improving the security of access to their email accounts.

Within the study, the holistic phrase was used, through a mixed and projective approach, where the methods of quantitative and qualitative collection were applied, with the purpose of establishing the problematic reality within the company. To this end, three users were interviewed with the respective positions of director, manager and head of the area, as well as audit records with user access from external and internal environments, users who handle information regarding the company and which service they use more if SharePoint or OneDrive, also these tools were directly related to the theoretical framework described within the research.

In conclusion, after carrying out the fieldwork and developing a triangulation between the data collected quantitatively and qualitatively, it was possible to diagnose that there were basic policies applied to the users of the company, identifying the solution problem that allowed a research proposal based on the application of security policies on mobile devices, authentication per user, improving data access control by mapping it by area, empower users to use their accounts and devices that have access to their information and documentation in order to improve the policies and control of the platform and sensitive data files belonging to the company.

Keywords: Information protection, security policies, Cloud office 365 platform.

Introducción

Actualmente las empresas a nivel nacional cuentan con muchas amenazas tecnológicas por las que podrían perder información, en su mayoría las empresas no tienen la infraestructura correcta de prevención o cómo actuar ante casos como este, generándoles inconvenientes en su trabajo como perdidas de información, vulnerabilidad, o casos de retención de información y llamadas de secuestro de datos.

Las empresas en Perú no invierten demasiado en la seguridad de la información por motivos de costo, falta de conocimiento del personal ante las amenazas actuales o de los datos sensibles que podrían estar en peligro, entre otras.

En las tendencias en el ámbito tecnológico empresarial y comercial se puede observar la necesidad de disponibilidad de la información y la colaboración, para esto utilizan sistemas o plataformas que les permitan utilizar estas funcionalidades, los correos y archivos con alta disponibilidad y de edición, aunque con este tipo de disponibilidad, nace la consulta. ¿Cómo protejo la información de mi empresa cuando se encuentra fuera del área perimetral? Los encargados de sistemas tienen la tarea de analizar un plan para la implementación de seguridad en los administradores donde se alojan los documentos sensibles y/o vulnerables, ello para mantener la confidencialidad y la integridad de la información de manera segura entonces cual sería el plan o proyecto para ejecutar que nos ayude a que los documentos tengan y se encuentren disponibles.

En la empresa Replica se utiliza Office 365 un portal en nube que nos brinda estas características, debido a casos de pérdidas de datos en el área comercial, optamos por realizar una mejora de seguridad, tanto de correos y/o archivos, para poder controlar de una manera eficiente y con reportes generados en una documentación, de tal manera a partir de este análisis e implementación reducir la amenaza en la data sensible de la empresa.

Con el anterior preámbulo, se define como la meta de este estudio elaborar e implementar una propuesta en la que apliquemos las políticas de seguridad de información en la plataforma en nube utilizada por la empresa comercial que nos permita mejorar la seguridad y los accesos de usuarios hacia la data de la empresa comercial que se ubica en Lima, Perú, de tal manera ir solucionando los problemas que parten de las políticas de seguridad de la información y que al final son perjudiciales por no estar documentadas y aplicadas.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Problema de investigación

Según datos y estimaciones de la rentabilidad muestran que la adopción de la nube aumentaría de una manera significativa entre 2012 y 2016, en forma particular en México y en Argentina. Se suman, Colombia y Chile que figuran entre los países de rápido crecimiento o evolución hacia los servicios en nube, según lo informado por la CEPAL. (Israel, 2016).

En el segmento del mercado nube y Gartner el software como servicio (SaaS) se refleja en un crecimiento del 22%, este año llego a los US$73.600 millones. De esta forma, las empresas estarán invirtiendo el 45% en SaaS para los software de aplicaciones para el 2021. (Aetecno, 2018).

No obstante, las actividades que se programaron, para consultoría informática y actividades conexas aumentaron en 5,29% por el mejor desarrollo de empresas relacionadas a gestión de negocios (e-commerce), en la investigación de implementación de un sistema de video vigilancia, cloud (computación en nube), data center, correos electrónicos, inteligencia artificial como chatbots (comunicación automática) y ciberseguridad, que se especializaron para empresas del sector bancario y retail; de la misma forma también el avance de las empresas de ingeniería informática como desarrollo de software, diseños y estructuras de páginas WEB y aplicaciones informáticas, que se impulsaron por la creciente demanda en transformación digital y agilización de las transacciones comerciales del sector telecomunicaciones, financiero y retail. (Zanabria, Sánchez Aguilar, & Montoya Sánchez, 2019).

Las nuevas tecnologías que emergen de manera exponencial dentro del ámbito comercial y empresarial nos han facilitado el acceso a la información tanto personal como empresarial, gracias a las nuevas plataformas de nube (Cloud Computing) facilitando su disponibilidad e integridad de la información hacia nuestros usuarios finales dentro de la organización, pero dentro de esta nuevas tecnologías nace la pregunta ¿Cómo protejo la información de mi empresa cuando se encuentra disponible en las plataformas de nube (Cloud Computing)?.

El personal de sistemas de las empresas debe estar preparados para poder administrar la seguridad de estas nuevas tecnologías y ver las funcionalidades proporcionas por las marcas para garantizar la propiedad de la información, tanto para la empresa como por parte de la plataforma en nube que están adquiriendo.

En este caso, nuestra muestra será la empresa Replica con una plataforma en nube de la compañía Microsoft denominada Office 365 que nos proporciona servicios de correo electrónico, almacenamiento en nube, gestor documental y centro de comunicaciones, dentro de la plataforma podemos encontrar herramientas para mejorar la seguridad y cumplimento de las políticas que implementaran el personal de sistemas, cabe mencionar que las herramientas de Office 365 se pueden complementar adquiriendo más Servicios de niveles superiores para un mejor rendimiento de los servicios.

1.2 Formulación del problema

1.2.1 Problema general

¿Cómo reducir el riesgo de la perdida de documentación en la empresa Replica dentro de la plataforma de Office 365 de sus usuarios?

1.2.2 Problema específicos

¿Cómo es la protección de la información en la empresa Replica?

¿Cuáles son los factores/causas de mayor inseguridad en la empresa replica?

¿Como las estrategias influyen en la seguridad de la información en la empresa Replica?

1.3 Justificación

1.3.1 Justificación teórica

La teoría General de sistemas nos ayudara en el trabajo de investigación en la implementación de las políticas de privacidad de los datos de la empresa, la teoría general de sistemas ayudara a determinar cuáles son los procesos que podremos segmentar. La teoría de las políticas de información nos ayudara a reducir las pérdidas de información evaluando los datos que se desean proteger.

De acuerdo con el tema de investigación determinamos mediante los conceptos en políticas de seguridad de información que incluyen las teorías de sistemas e información se busca proponer políticas para regular las políticas de seguridad, de esta manera podemos indicar los factores de riesgo y aumentar la seguridad de los documentos empresariales en la empresa Replica.

1.3.2 Justificación metodológica

Se determina utilizar el estudio de investigación holística que usará un enfoque mixto, presentando un estudio para obtener resultados acertados que nos permitirá asegurar los procesos correctos, de tal manera determinar las causas y efectos sobre la información corporativa que utilizan los empleados, y esto nos permitirá obtener una solución propicia para mejorar la seguridad de los archivos corporativos.

La investigación que realizamos nos ayuda reducir el riesgo de la perdida de información aumentando la seguridad de los datos corporativos, y tener un mejor control sobre los datos que se comparten, o accedan desde cualquier lugar que pertenezcan a la empresa.

1.3.3 Justificación practica

La investigación que realizaremos para implementar políticas de seguridad que permitan aumentar la confiabilidad de la información, para ello los procedimientos en el uso de la plataforma tendrán relación con el objetivo de esta manera mantener un uso adecuado con seguridad en los datos a los que el usuario tiene acceso. Por otro lado, revisamos que los accesos hacia la información corporativa sean con métodos adicionales de autenticidad será útil ya que nos permitirá mejorar la seguridad de la información corporativa que se comparte desde la plataforma nube, agregando políticas de seguridad, agregando protocolos determinados incluyendo esto aumentara el control de la información corporativa utilizada por la plataforma nube, que nos permite almacenar archivos y compartirlos.

1.3.4 Limitaciones

Falta de conocimiento de las herramientas de seguridad.
Compatibilidad de software y hardware
Falta de apoyo de los usuarios involucrados en los procesos
Cantidad de trabajadores en la empresa Replica S.R.L.

1.4 Objetivos

1.4.1 Objetivo general

Proponer políticas de seguridad de la información para proteger la data sensible que utilizan en la empresa Replica

1.4.2 Objetivos especifico

Analizar las políticas de seguridad en la empresa Replica S.R.L
Explicar las causas de mayor inseguridad de la información en la empresa Replica.

CAPÍTULO II

MARCO TEÓRICO

2.1 Sustento teórico

Teoría General de Sistemas

T.G.S. se denomina una filosofía o un método que se utiliza como apoyo para analizar y evaluar el contexto actual y los modelos de desarrollo, de esta manera se intentara una aproximación progresiva para la apreciación del global que conforma el universo, esto forma un modelo que no se aísla, es llamado sistema (Sarabia, 1995).

Una metodología o estructura con propósito de que estudia el sistema globalizado de manera íntegra, su base con los componentes de acuerdo con eso procede a analizar las relaciones e interrelaciones que existen, por medio su aplicación como estrategias científicas, esto se dirige a la comprensión que globaliza y generaliza el sistema (Tamayo, 1999).

Se plantea que la teoría general de los sistemas es: “Una ciencia general de la “totalidad”, este concepto viene concebido hasta hace poco por simple, nebuloso y semimetafísico. planteando su elaboración sería una seria una disciplina lógico-matemática, puramente formal de tal manera que actúa en sí misma, pero logra ser aplicable a las varias ciencias empíricas” (Von, 1976).

Con el propósito de mejorar las políticas de la seguridad de información usaremos el contexto de la teoría de sistemas, de tal manera nos permitirá determinar el proceso en cual enfocarnos para encontrar la solución idónea, podemos indicar que la teoría de sistemas se separa en dos partes, lógica y matemática, que podemos interpretar como aspectos demostrativos que se aplican en otros aspectos de la realidad.

Teoría General de la información

La teoría de la información se ocupa del enfoque social y las comunicaciones colectivas como una amplia disciplina. Es denominada una nueva, básica e indispensable ciencia que ayuda a

comprender los fenómenos contemporáneos que en la actualidad se denomina comunicación por masas. (Benito Jaén, 1981)

Los cambios en los medios de comunicación como el procesamiento de información en la mitad del siglo son tanto en difusión como especialización que construyeron el primer el modelo científico del proceso que se conoce como teoría de información, también llamada teoría matemática de comunicación. Se especifica el desarrollo de la telegrafía que nace para determinar una necesidad, con precisión, los diferentes sistemas son capaces de transmitir información (López, Parada, & Simonetti, 1995).

Teoría General de la gestión de Riesgo

La teoría general de gestión de riesgo se define como el "conjunto de medidas administrativas, organizativas y conocimientos operativos para aplicar políticas y estrategias con el objetivo de reducir o mitigar el impacto de las amenazas naturales y desastres ambientales y tecnológicos" (Chuquisengo, Pinedo, Torres, & Rengifo, 2005)

La gestión del riesgo se puede concebir como el grupo de elementos, medidas y herramientas que se orientan a controlar la amenaza o la vulnerabilidad, que es aplicado como propósito de reducir los riesgos de desastre. Sus distintos tipos de acción tienen la intención de relacionarse, para facilitar un rol primordial la de prevención y reducción sin dejar de lado la preparación para tener una respuesta en caso suceda algún desastre (Cardona, 2003).

Con el propósito de aumentar la seguridad de la información, utilizamos la teoría general de gestión de riesgo, para poder actuar antes de que sucedan infortunios, generando políticas de seguridad que controlen y reduzcan las amenazas en la empresa comercial.

2.2 Antecedentes

Bermúdez y Bailón (2015) en el análisis en seguridad informática y la seguridad informática que se basa en la norma ISO/IEC 27001, en los sistemas que gestionan la seguridad de

información que se dirige a una empresa de servicio financieros, indicando como objetivo principal analizar los procesos críticos de la empresa Credigestión con respecto a tramites de seguridad para respaldar la confidencialidad, integridad y disponibilidad de la información, se formularon recomendaciones en seguridad y controles basados en la ISO/EIC 27001, La metodología holística utilizada se alinea a las normas de la ISO/IEC 27001, se enfoca en la seguridad de la información, se empezó con el reconocimiento de las vulnerabilidades, conflicto y amenaza de los activos de información que influyen en los departamentos críticos de Credigestión. En el análisis de este antecedente se determinó que la información se encuentra propensa a daños, robos o modificaciones por las acciones involucradas en los procesos de la empresa con esto se podrá encontrar puntos de riesgos en la seguridad de la información.

Vasquez (2016) en la apreciación de la gestión de Ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, 2016, su fin fue determinar la gestión de la seguridad para la prevención de los ataques cibernéticos en las pymes del Perú, 2016. Mediante la metodología holística que fue aplicada en el análisis, obtuvieron los resultados que se derivaron de la encuesta en la que se demostró que para el personal consultado de la empresa Transporte Zavala Cargo S.A.C. la ciberseguridad no está implementada ya sea en políticas y procedimientos, es importante realizar la implementación para orientarlas a buenas prácticas de acuerdo a las normas en el uso de la tecnología, los usuarios no están formados con respecto a la ciberseguridad, de esta manera no evitan las amenaza, sin invertir en ciberseguridad, ni un responsable de seguridad de la red.

Alcántara (2015) el trabajo desarrollado con título Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, de esta manera apoyar la seguridad de los sistemas informáticos de la comisaría del norte P.N.P., Chiclayo, con la finalidad de contribuir en la mejora del nivel de seguridad de la información. Que será apoyado por la norma ISO/IEC 27001, en la institución policial comisaría del norte – Chiclayo, se realizaron encuestas de los que el resultado fue conocer los entregables que se asocian a la norma ISO/IEC 2700, estos se resumieron en entregables.

2.3 Marco conceptual

Gestión de Seguridad

Los riesgos de la seguridad de información se tratan de conocer, minimizar, asumir para que se gestionen por las entidades de negocio de forma que se documente, estructure, repita, de forma sistemática, para adaptar a los cambios que se produzcan en casos de riesgo en diferentes entornos y por medio de distintas tecnologías. En el desarrollo de esta propuesta es fundamental el uso de una gestión de seguridad dado que se empleará en la plataforma, ello nos permitirá tener control sobre la información corporativa, bases datos de clientes, entre otros (Rayme, 2007).

Se trata del desarrollo de un procedimiento lógico y por periodos, se basan en la mejora continua; que engloba la política, la aplicación, la evaluación, y los cambios de mejora, con el propósito de anticipar, examinar, evaluar y comprobar los riesgos que perjudiquen la seguridad en la empresa. Este concepto es fundamental porque el servicio que se brindará tendrá como uno de sus objetivos la idoneidad de la información por ser el eje principal del servicio propuesto (Ojeda, 2017).

Subcategoría Ataques Informáticos

En la actualidad se conoce a los ataques informáticos como una de las amenazas más grandes para las empresas. ya que afecta a usuarios, empresas, incluso a estados y sociedades. Las medidas de seguridad informática tienen prioridad en empresas o entidades que dependen del uso de casi un 100% de internet para realizar operaciones, ya sean transacciones o compartir documentos importantes para la empresa (Optical Network, 2019).

Las amenazas informáticas que se basan en internet tienen una evolución gradual, se ha convertido en una preocupación constante para personas y empresas que necesitan mantener su información intacta, ya sea de dispositivos o información de diversos indoles, según un estudio de Kaspersky Lab, de seguridad en tecnologías de la información (TI).

Reflejo un 82% de las empresas sufrió de uno a cinco intentos de ataque, el 10% de estas sufrió pérdidas de datos y de accesos a la información aproximadamente una semana, el 15% sufrió impedimento de transacciones comerciales.

Suplantación

Se conoce como apropiación ilegal de identidad. Este fenómeno delictivo afecta en algunos casos de manera inmediata a las víctimas que lo padecen, y en otros casos las consecuencias se manifiestan a largo plazo, ejemplo de ello, cuando una persona utiliza la identidad de otra para realizar una solicitud de crédito, procedimiento que es desconocido por la víctima, pero a mediano plazo ésta empieza a recibir notificaciones de la deuda existente por un crédito que jamás solicitó, o en casos extremos le es comunicada que es perseguida por la justicia. (Visión Criminológica-Criminalística, 2013)

La parte afectada en esta problemática sin lugar a duda es la víctima, quien pierde de manera específica, su identidad legal, su estabilidad económica, en casos extremos su libertad, y principalmente se encuentra ante un inevitable daño moral, donde su prestigio o su imagen se ven completamente dañadas ante los ojos de la sociedad o de la justicia.

Phishing

Phishing es un conocido con el término informático utilizado para denominar el fraude por suplantación de identidad, una técnica de ingeniería social. Este se originó de la palabra phishing se dice que proviene de la contracción de “password harvesting fishing” (cosecha y pesca de contraseñas); cabe mencionar, que la explicación es muy probable que sea posterior al propio término. El término phishing procede de la palabra inglesa “fishing” (pesca) haciendo alusión a caer en la trampa. (Núñez, Villaroel, Cuevas, 2010)

Este término fue utilizado por primera vez en 1996, en los casos en que se intentó apropiar de cuentas de AOL, a pesar de que se había iniciado varios años antes. Se refería a

envío de mensajes instantáneos haciéndose pasar por empleados de AOL, en los que solicitaban contraseñas. AOL tomó medidas en el año 1995, y reforzó las mismas en 1997.

También podemos ver en generación de tráfico utilizando un origen falseado, suplantación de usuarios en una comunicación en red. Personas que suplantaron una identidad de un objetivo específico.

Spoofing

El spoofing se trata de una suplantación de identidad, pero en la cual no se requiere por lo general de un engaño previo a la víctima o a la entidad. Adicionalmente, los motivos de este pueden ser muy variados, desde la estafa a la investigación. (Núñez, Villarroel, Cuevas, 2010)

Como cabe mencionar, normalmente el spoofing no usa el engaño, por lo que la actuación de forma general es básicamente técnica, menos picaresca y fraudulenta. Por tal motivo esto requiere siempre de unos conocimientos muy avanzados.

Subcategoría Control de políticas

El control es como un enfoque metódico de análisis y planeamiento de controladores, que se fundamentan en el uso de la matemática. Se usan conceptos para la función de claridad, que vincula la salida y entrada de un método característico para evaluar sus propiedades (Fermín, 2011).

El control es una rama interdisciplinaria de la ingeniería y de las matemáticas, se trata como practicas dinámicas, estas dependen y comparten herramientas con la física, los equipos de escritorio, la investigación operativa y la IA, de las cuales se vacían instrumentos y metodologías que nos permita ampliar la posibilidad del control (UCM)

Se trata del caso en que el acceso de un administrativo cambia datos que pueden ser obstáculos que impiden realizar una acción o actividad particular, que no se trata de un privilegio, ayuda a la mejorar la eficiencia de los casos (Delgallo, 2005).

Administrador Global

La tendencia de la administración de roles que siguen los proyectos está cambiando. Los roles se consideran como beneficiosos por derecho propio, y complementan otras iniciativas. Las organizaciones están descubriendo que la administración de roles requiere una inversión significativa en esfuerzo inicial, incluyendo descubrimiento, la definición, y la administración del ciclo de vida de los roles, por lo que legítimamente cuestionan el valor de la inversión. La comunidad de los estándares ha establecido definiciones teóricas; las pautas prácticas de la implementación son obras en fase de creación.

Este tipo de rol de administrador nos permite controlar y dar acceso a otros usuarios, también extraer los logs de auditoria y poder tener la data organizada.

Administrador Personalizado

Este rol nos permite designar a un encargado por portal, no tendrá todos los accesos ya que su portal es personalizado, de esta forma tiene un orden y se encarga de las tareas designadas. Como la administración y permisos del portal que es asignado por el administrador global.

Usuario

El rol de usuario tiene su plataforma para el uso de sus licencias y configuraciones personalizadas, con el acceso a los servicios que se otorguen por la licencia asignada. El usuario será notificado de los archivos a los que tiene accesos y si tienen permiso de lectura o escritura.

Subcategoría Accesos de información

Al presentar el concepto de la informática revisamos que es aplicable y teórico, como resulta ser en diferentes estudios ya sea en computación y diferentes ramas en las que se aplican estos conocimientos. Se evalúa la estructura, pautas e interacciones de sistemas naturales y las tecnologías de la información. Se abordan diferentes esquemas para comprender los problemas en los que se aplican las tecnologías de información de la manera en la que sea necesaria (Cañedo, Ramos & Guerrero, 2005).

Se conoce como disciplina que integra, emana de las aplicaciones con diferentes ciencias, ya sea electrónica, cibernética, matemática, lingüística, AI inteligencia artificial, se estudian los progresos, servicios, procedimientos, arquitecturas de la comunidad de informática.

Permiso de accesos

Un control de accesos es un dispositivo o aplicativo que tiene por objeto impedir el libre acceso del público en general a diversas áreas o aplicaciones que denominaremos protegidas.

Por lo tanto, lo primero que se debe identificar, para justificar la instalación de un control de accesos, es la existencia de elementos que se desean proteger. En una empresa o comercio estos elementos a proteger pueden ser fácilmente identificables, como los archivos donde se manipula dinero, donde se guardan los registros del personal y bases de datos, entre otras, y algunas no tan obvias. Se deben proteger con contraseñas seguras PIN u otro método de autenticación.

Lectura

El tipo de acceso a la información en modo lectura, nos permite controlar la edición del archivo, este modo solo estará activo para usuarios que no necesiten editar, como listas de precios y o algún manual enviado por áreas respectivas para la información.

Escritura

El tipo de acceso de escritura es otorgado a usuarios que necesiten modificar algún archivo, este tipo de permiso, será en documentos que no se deban descargar, teniendo como evaluación si es un documento con contenido sensible de la empresa. Evitando perdidas de información.

Riesgos

La sociedad del riesgo es nueva manera social que brota como resultado de la actualización de la sociedad industrial. De acuerdo con esta pauta, el origen de esta apariencia social no se elabora por un estallido político, de tal manera es la consecuencia de la modernización. Dentro de la implementación se tendrá en cuenta el desenvolvimiento de los usuarios para poder mitigar los riesgos que puedan originarse con el uso inadecuado de la información (Albarracín, 2002).

Un proceso de gestión de riesgo debe permitir que la organización entienda cuál es su situación actual de seguridad, le facilitara tomar decisiones para mitigar los riesgos; de la misma forma evaluar que las medidas que se implementen a largo y corto plazo, al final especificar si las decisiones fueron las correctas. (Guevara, 2012).

Respaldo de cuentas

En general, un respaldo es una copia con data que una organización genera, utiliza y actualiza a lo largo del tiempo; también empleamos este término para las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, software de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia. (Benavides, 2016)

Normalmente, los respaldos se llevan a cabo en unidades de almacenamiento secundario, como discos duros externos, memorias flash, discos compactos, cartuchos e incluso en la nube (Internet) o en otros equipos de cómputo, locales o remotos.

Buzones de correo

Un buzón de correo también se denomina cuenta de e-mail. El buzón de correo electrónico recoge todos los correos electrónicos que el usuario ha enviado y recibido desde y hacia su dirección de correo electrónico. Cada buzón de correo electrónico tiene una dirección de correo electrónico por defecto. Para acceder a este buzón necesita una dirección de correo electrónico, así como un programa de correo electrónico como Webmail, Outlook o una aplicación para smartphones. (Sainz-Aloy & Soy-Aumatell, 2011)

Cada buzón de correo electrónico tiene un espacio de almacenamiento específico en el que se almacenan los correos electrónicos. El tamaño de este espacio de almacenamiento depende del proveedor y de la tarifa - no existe una regulación uniforme. Los correos electrónicos enviados y recibidos se almacenan allí hasta ser eliminados por el usuario.

Log de auditoría

Los logs de auditoria nos permiten identificar eventos de interés, que pueden suceder frente a una pérdida de archivo o consulta de algún permiso creado, etc. Las tecnologías de que nos permiten obtener los registros y la información de dichos eventos deben estar protegidos contra posibles adulteraciones, o accesos no autorizados. Se debe tener un control para proteger de cambios no autorizados. (Sistema de Gestión Integrado, 2017)

Autenticador de Usuarios

Cuando utilizamos un servicio con nuestro usuario y contraseña, estamos utilizando dos datos que en teoría sólo sabemos nosotros. el inconveniente es cuando, esta contraseña no siempre es segura, para evitar ese escenario, añadimos otro factor para poder acceder al servicio,

configurado con algo que utilizamos siempre. podemos utilizar nuestro dispositivo móvil el cual nos ayudara con la generación de un clave token puede enviarse por mensaje o utilizar un aplicativo para generarla, por tal motivo sería mucho más seguro los accesos ya que se corrobora la identidad del usuario. (Marqués, 2017)

Aplicaciones

Una aplicación informática es un tipo de software que permite al usuario realizar uno o más tipos de acciones ya sea para el trabajo o distracción. Son, aquellos programas que permiten la interacción entre usuario y computadora o dispositivo móvil, dando opción al usuario a elegir opciones y ejecutar acciones que el programa le ofrece. Existen innumerable cantidad de tipos de aplicaciones, mientras que los sistemas operativos o los programas de utilidades (que cumplen tareas de mantenimiento) no forman parte de estos programas. Las aplicaciones pueden haberse desarrollado a medida (para satisfacer las necesidades específicas de un usuario) o compatible con un sistema operativo. (Fernández-Pinto, López-Pérez,, & María, 2008).

2.4 Empresa

2.4.1 Descripción de la empresa

La empresa REPLICA soluciones tecnológicas, es una empresa de 24 años con experiencia en la tecnología de la información, se compromete a brindar un servicio de alta calidad. Su amplia cartera es su carta de presentación.

REPLICA inicio sus operaciones en el año 1994, desde entonces brinda productos y servicios de última generación, siempre brindan soluciones integrales de software y hardware, capacitación de proyectos con tecnología de punta.

Va de acuerdo con el crecimiento tecnológico y siempre apuesta por las ultimas tecnología, con constante actualización.

2.4.2 Marco legal de la empresa

La empresa Replica S.R.L es una organización tipo contribuyente sociedad comercial de responsabilidad limitada, como se muestra en la siguiente figura:

Figura 1. Datos generales de Replica S.R.L.

Fuente. Sunat.

2.4.3 Actividad económica de la empresa

La empresa REPLICA en la actualidad cuenta con actividad económica al brindar otras actividades de tecnología de información y servicios informáticos, la cual tiene como objetivo brindar soluciones tecnológicas a las empresas; así mismo se brinda actividades de venta al por menor en comercios no especializados, y enseñanza superior.

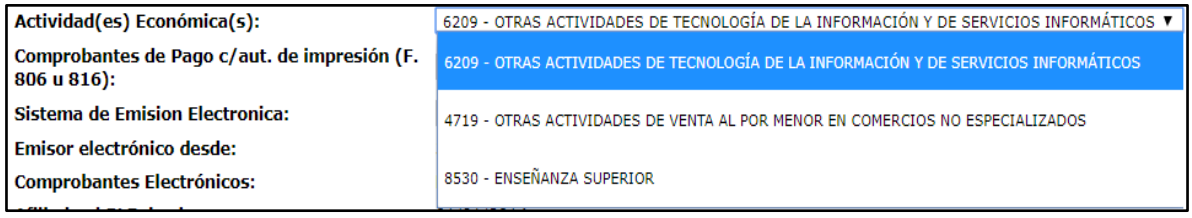


Figura 2. Actividades económicas de Replica S.R.L

Fuente. Sunat.

2.4.4 Información tributaria de la empresa

RUC 20251505111

Nombre de empresa Replica SRL.

2.4.5 Información económica y financiera de la empresa

Le ha dado la autorización a Replica S.R.L. para realizar y generación de los siguientes documentos mostrados en la figura.

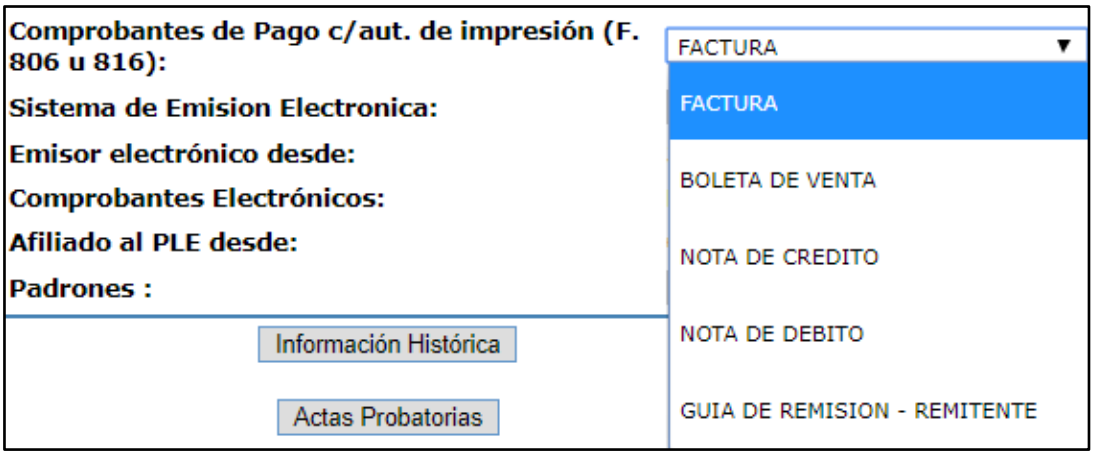


Figura 3. Comprobantes de pago de Replica S.R.L

Fuente: Sunat

2.4.6 Proyectos actuales

Se está realizando la implementación de un gestor documental que ayude a compartir la información con los clientes de la empresa Replica, para brindar capacitaciones.

Creación de una mesa de ayuda utilizando SharePoint, para la facilidad de comunicación con los clientes.

Empoderar a los clientes con productos y servicios de tecnología.

Impulsar el Área de Marketing Digital

Impulsar el Área Tecnológica de Proyectos

Impulsar el Área de Capacitaciones en Línea

Impulsar el Área de Diseño y Desarrollo

2.4.7 Perspectiva empresarial

Misión

Brindar la mejor asesoría a los empresarios, con su crecimiento es un logro más para nosotros.

Visión

Tener reconocimiento de nuestro crecimiento en las soluciones de tecnología y con servicios innovadores en la gestión para la eficiencia de las empresas.

CAPÍTULO III

MÉTODO

3.1 Tipo, nivel y método

Enfoque

Este enfoque nos permite evaluar el nivel del problema de la investigación. Podemos determinar cuáles son nuestros puntos de dificultad, como en nuestros procesos que utilizamos para la investigación y en cada etapa de nuestro desarrollo. (Hernández, Fernandez, Baptista 2010).

Nos ayudará a responder nuestro planteamiento del problema, utilizando la data recolectada de método cualitativo y cuantitativo, con estos datos podremos determinar los mejores procesos para brindar una solución para nuestra empresa.

Tipo

Esta propuesta es con un estudio proyectivo, se realizará la mejora en la protección de la información.

El estudio proyectivo se usa con la mejora de procesos comprendiendo los estudios determinando la mejor solución que se podrá utilizar, se revisaran las condiciones donde aplicar los casos realizando pruebas y con un seguimiento de las mejoras propuestas, esto nos permitirá prevenir sobre la realización del proyecto, construcción y modificación de mejoras (Hurtado, 2000).

Nivel

Nivel utilizado para esta aplicación será de carácter comprensivo, nos ayudará a evaluar directamente las relaciones entre los procesos y determinar con un sintagma holístico como comprender y definir la realidad para la posible solución. En la medida que nos permite estudiar el todo a través de las partes nos ayudará a proponer un modelo con mayor precisión a la problemática (Hurtado, 2000).

Método

Los métodos inductivos y deductivos se les conoce por tener diferentes fines que generalmente son clasificados como desarrollo de la teoría y estudio de la teoría determinadamente. Los métodos inductivos se han mostrados generalmente asociados a la investigación cualitativa en cambio el método deductivo se muestra generalmente con la investigación cuantitativa. (Abreu, 2014).

3.2 Categorías y subcategorías apriorísticas

Tabla 1.

Categorización de gestión de seguridad

Categoría	**Subcategoría**	**Indicadores**
Gestión de Seguridad	Ataques Informáticos	Suplantación
		Phishing
		Spoofing
	Control de políticas	Administrador Global
		Administrador Personalizado
		Usuario
	Accesos de información	Lectura
		Escritura
		Permiso de accesos

Fuente: Elaboración propia

Tabla 2.

Categorías emergentes

Categoría	Subcategoría	Indicadores
Gestión de Seguridad	Respaldo de cuentas	Buzones de correo
		Log de auditoria
		Accesos de cuenta
	Autenticador de Usuarios	Accesos
		Aplicaciones
		Usuario

Fuente: Elaboración propia

3.3 Población, muestra y unidades informantes

Población

La particularidad de los casos que suscitan bajo un conjunto de ellos es la población, que se determina de acuerdo con especificaciones. (Hernández, Fernandez, Baptista 2010).

Para nuestra investigación seleccionaremos una población con un tema relacionado entre sí, esto nos ayudara enfocándonos en el objetivo.

Tenemos en consideración los registros de auditoría que se obtendrán de los accesos a los buzones de correo de los trabajadores de la empresa Replica S.R.L, contamos con los registros que nos brinda la plataforma de un rango de tres meses de los que evaluaremos los accesos a sus cuentas de correo y los accesos a la información.

Muestra

El grupo que se caracteriza por el tamaño es la muestra. Utilizando características para analizar los resultados de grupo, nos permitirá conseguir la información solicitada mediante métodos de obtención ya sea por encuestas o utilizando cuestionarios. Los análisis de dichos usuarios se obtendrán de manera aleatoria para aplicarlas en este proyecto (Arias, 2012).

Se definieron los cuales serán los colaboradores de la organización para participar, analizares características de las frecuencias con las que utilizan la información corporativa, las cuentas de usuarios corporativos. Utilizaremos los usuarios con mayor frecuencia de acceso y realizar una investigación de ataques, ya sea por malos registros u otras vulnerabilidades. Esta población nos ayudará con la recolección de datos y nos facilitará cumplir nuestro objetivo.

Unidades informantes

Se debe tener en cuenta cuales son los usuarios a los que entrevistaremos, ya que por medio de esta información recolectada verificaremos si tenemos fallas en nuestras políticas de seguridad y revisar si el área requiere mejorar la seguridad de la información. (Hernández, Fernández & Baptista, 2010).

En el estudio se deben segmentar o identificar bien las unidades informantes ya que estas nos guiaran con la investigación de tal modo que se verifique la factibilidad de la investigación.

3.4 Técnica e instrumento

Uno de los procedimientos que aplicaremos a nuestra propuesta es la recolección de datos, esto nos permitirá recolectar la información necesaria que nos facilitará la evaluación de esta manera obtener las respuestas de nuestras incidencias mencionadas con anterioridad. (Hurtado, 2000).

La investigación cualitativa es la que elabora datos descriptivos, con las palabras propias de cada persona, ya sea escrita o hablada y el comportamiento observable. Que compone un conjunto de técnicas para acumular datos. (López & Sandoval, 2013).

La investigación cuantitativa se fundamenta con técnicas mucho más ordenadas, ya que busca medir las variables establecidas con anterioridad. (López & Sandoval, 2013).

La entrevista es una de las habilidades preferidas de los seguidores de la investigación cualitativa, pero también es un método muy usado por los siquiatras y otros profesionales, que a la postre es una de las formas de la interrogación, o sea el preguntar a alguien con la voluntad de obtener de información específica. A este apartado de la interrogante pertenece también además de la entrevista, el cuestionario, que a diferencia de la primera es escrita. (Cerda, 1991).

El cuestionario es solamente una herramienta para almacenar datos con la finalidad de usar en un estudio. Primero debemos tener claro qué tipo de estudio queremos realizar, para entonces poder decidir si nos puede resultar útil usar un cuestionario. (Fernández, 2007).

Instrumento

Este instrumento nos ayuda en cómo proceder con el grupo definido de estudio con las interrogantes determinadas de la investigación que deseamos conocer algo" (Sierra, 1994), puede tratarse de un plan, una forma de entrevista o una herramienta de cálculo. Aunque el cuestionario puede ser un procedimiento escrito para lograr datos, es posible adaptarlo verbalmente. (Corral, 2010).

Validez

El proceso de la acumulación de pruebas que nos ayuden a interpretar la relación frente a un objetivo, que se puede interpretar de forma explícita de fundamentos teóricos y predicciones que se justifican científicamente. (Prieto & Delgado, 2010)

Utilizamos la validez para medir la confiabilidad de nuestra investigación, revisando la información encontrada y los resultados de los análisis de datos realizados.

Confiabilidad

Los datos deben haber sido obtenidos por un instrumento de forma determinada por condiciones generales o bajo condiciones que se determinaron en un inicio una forma de probarlo sería medir bajo un mismo rango de condiciones. (Ruiz, 2015)

La confiabilidad se aplicará en nuestra investigación determinando las condiciones bajo las cuales podamos obtener los resultados que podamos volver a medir bajo los mismos parámetros que el inicial.

3.5 Procedimiento

Los pasos que se seguirán dentro del presente estudio parten por determinar los procesos que realizan los usuarios por medio de la acumulación de los datos recolectados cuantitativos por medio de instrumentos mencionados con anterioridad para obtener datos y realizar nuestro estudio con la encuesta, en la obtención de datos cualitativos tenemos a la entrevista.
Usaremos la gestión de archivos, recopilaremos información de la plataforma, revisando los ataques a cuentas, e indicando cuántos archivos se comparten al día sin protección de la información, de esta manera tendremos el estudio de lo que mejoraremos.

Cuantitativo

Es uno de los análisis más importantes que pueden llegar a darnos la información para responder en los objetivos que se plantearon para la investigación, podemos aplicarla de maneras distintas como descriptivo o inferencial, generalmente se obtiene como una estructuración numérica de una o distintas variables y de esto se verán los tipos de análisis a practicar (Ruiz, Borboa, Rodríguez, 2013)

Usaremos el tipo de análisis cuantitativo para nuestro estudio, uno de estos tipos es la recolección de datos que aplicamos, para evaluar cómo se encuentran los accesos en nuestro portal, y como manejan la información los usuarios de la empresa.

Cualitativo

Al aplicar en nuestra investigación el análisis cualitativo, es utilizar a los implicados en el estudio para comprobar lo que sucede en su entorno, podemos obtener resultados de entrevistas, como describen su rutina de vida y de otros tipos de análisis (Ruiz, Borboa, Rodríguez, 2013)

Al aplicar el análisis cualitativo en nuestra investigación nos daremos cuenta si los administradores de la plataforma de la empresa Replica requieren de la solución que se plantea, para mejorar la seguridad de la información.

Mixto

El proceso del enfoque mixto nos ayuda con la recolección, análisis y vinculación de los datos cuantitativos y cualitativos en un mismo estudio lo cual nos permite responder a un planteamiento a través de una serie de investigaciones (Ruiz, Borboa, Rodríguez, 2013).

Se puede determinar que el enfoque mixto sería el apropiado, debido a que el enfoque cuantitativo nos facilitó incursionando en forma práctica en el juego de los números, tratamos la información empíricamente desde su origen, en la que se preparamos como primera instánciala recolección de datos que en nuestro caso es un log de auditoria, las cuales tienen variables dependientes e independientes de la investigación las cuales ligamos de una manera intima a los objetivos, con ello, se pretendemos usar estos resultados para conocer la percepción de los usuarios de la empresa Replica y poder corroborarlos con el Atlas TI.

3.6 Análisis de datos

La siguiente investigación busca el efecto entre las varias cuantitativas, con la finalidad de ver la relación entre las dos variables probando la independencia estadística, buscando el coeficiente de correlación, usando los datos recolectados con la finalidad de medir el efecto entre estas.

Análisis de datos es primordial en todos los tipos de evaluaciones. Este estudio nos muestra una perspectiva universal de los temas en relación la alternativa y uso de procedimientos para las estimaciones de impacto, es decir, las evaluaciones ayudan a proporcionar datos sobre los impactos a un amplio plazo presentido y no presentido que se produjo por los sistemas o políticas (Peersman, 2014).

Al obtener la información por medio de la gestión de archivos utilizaremos el diagrama de Pareto que nos permitirá evaluar la información cuantitativa.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Descripción de resultados

Análisis Cuantitativo

Tabla 3.

Lista de usuarios con cantidad de inicios de sesión

usuario	inicios
user14@replica.com.pe	2780
user5@replica.com.pe	2187
user15@replica.com.pe	1776
user25@replica.com.pe	1585
user1@replica.com.pe	1521
user50@replica.com.pe	1376
user13@replica.com.pe	985
user4@replica.com.pe	843
user24@replica.com.pe	790
ventas1@replica.com.pe	660
ventas2@replica.com.pe	606
user21@replica.com.pe	498
ventas4@replica.com.pe	497
user22@replica.com.pe	444
user6@replica.com.pe	442
user11@replica.com.pe	423
ventas@replica.com.pe	417
user12@replica.com.pe	384
user8@replica.com.pe	367
user17@replica.com.pe	325
user9@replica.com.pe	321
ventas7@replica.com.pe	266
user13@replica.com.pe	251
User@replica.com.pe	236
user7@replica.com.pe	232
user19@replica.com.pe	178
user2@replica.com.pe	160
user3@replica.com.pe	124
user16@replica.com.pe	27
user18@replica.com.pe	20
user10@replica.com.pe	1
user20@replica.com.pe	1

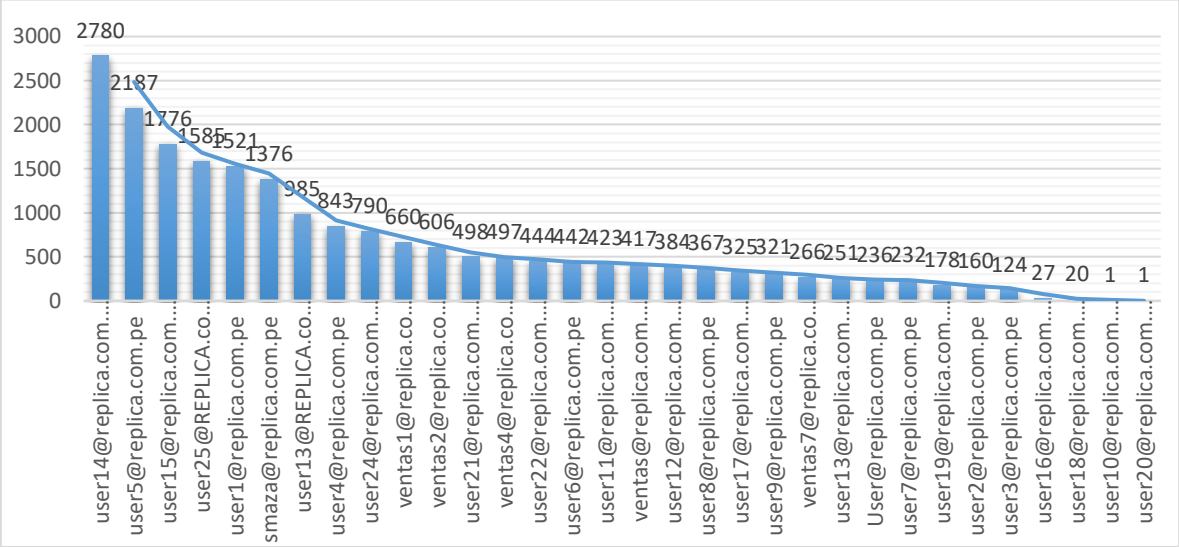


Figura 4. Inicios de Sesión Por usuario

Fuente: Elaboración propia.

En este grafico podemos revisar que 06 usuarios utilizan sus cuentas de correo con mayor afluencia, tanto dentro como fuera de la organización. Indicamos que 05 usuarios son administradores del portal, los cuales identificamos por los accesos cotidianos al sistema. Mientras que 01 usuario accede con mayor continuidad a la información de la organización tanto fuera como dentro de la empresa.

Tabla 4.

Lista de usuarios con cantidad de inicios de sesión

Etiquetas de fila	*Cuenta de Usuarios*
Acceso externo	17959
Acceso interno	2764
Total general	20723

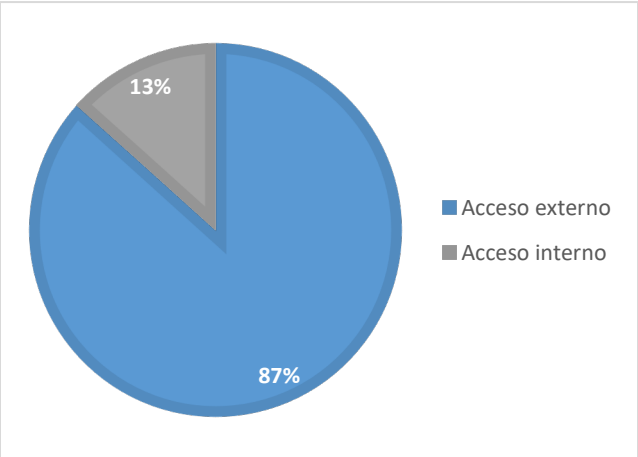


Figura 5. Inicios de Sesión Por usuario

Fuente: Elaboración propia.

En el gráfico se muestra que el 87% de los usuarios se conectan externamente porque utilizan las aplicaciones móviles de Office 365 y el correo vía web (OWA), los cuales están fuera de la red de internet de la empresa, mientras el 13% accede dentro de la red de internet de la empresa.

Tabla 5.

Registro de actividades.

Etiquetas de fila	false	true	Total general
asistente@replica.com.pe	154	6	160
bi@replica.com.pe	117	7	124
elaborador@replica.com.pe	1		1
ventas@replica.com.pe	394	23	417
ventas1@replica.com.pe	639	21	660
ventas2@replica.com.pe	594	12	606
ventas7@replica.com.pe	257	9	266
user1@replica.com.pe	790		790
user2@replica.com.pe	1618	158	1776
user3@replica.com.pe	293	28	321
user7@replica.com.pe	684	301	985
user6@replica.com.pe	1269	107	1376
user8@replica.com.pe	1478	709	2187
user4@replica.com.pe	2780		2780
user5@replica.com.pe	682	839	1521
user12@replica.com.pe	364	20	384
user17@replica.com.pe	1409	176	1585

profesor@replica.com.pe		27	27
user80@replica.com.pe	479	18	497
user30@replica.com.pe	481	17	498
user29@replica.com.pe	406	17	423
autodesk@replica.com.pe	830	13	843
user27@replica.com.pe	432	12	444
user28@replica.com.pe	227	5	232
user31@replica.com.pe	442		442
user32@replica.com.pe		178	178
user35@replica.com.pe	325		325
user37@replica.com.pe	362	5	367
user33@replica.com.pe	189	47	236
user34@replica.com.pe	243	8	251
user36@replica.com.pe		1	1
user38@replica.com.pe	20		20
Total general	17959	2764	20723

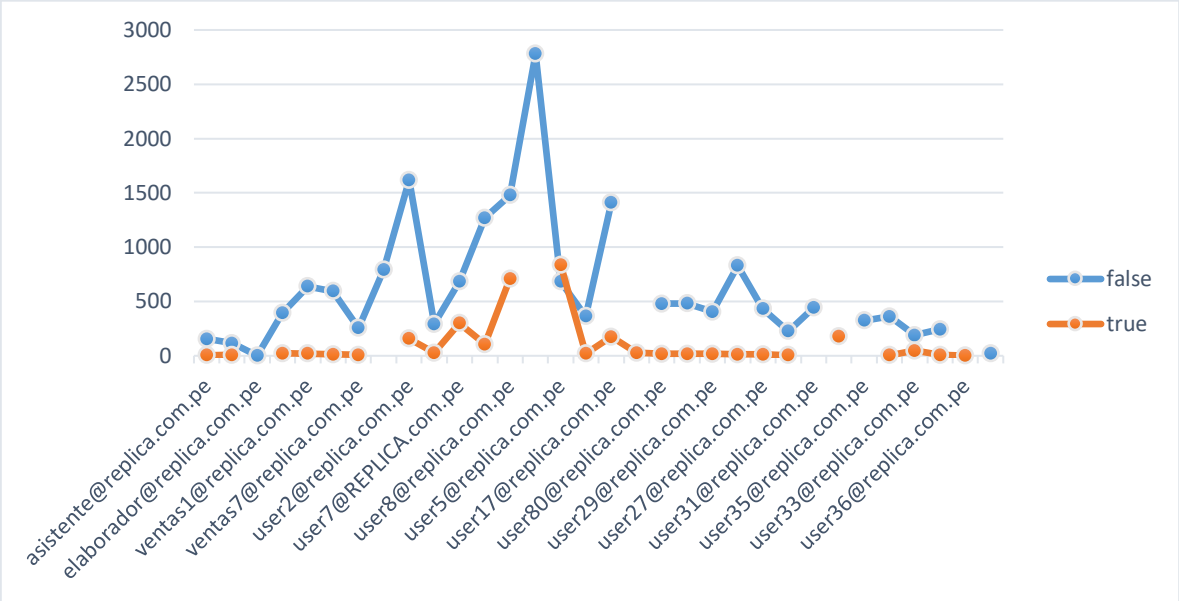


Figura 6. Accesos externos e internos

Fuente: Elaboración propia.

Según el grafico, visualizamos que los usuarios user6 y user1, cuentan con mayor acceso externo, ya sea por conexiones IP externas ya sea por reunión o accesos desde sus hogares.

Mientras que el user4, cuenta con mayor afluencia desde el rango incluido dentro de la empresa.

Tabla 6.

Registro de usuarios

Cuenta de Operaciones	Etiquetas de columna		
Etiquetas de fila	OneDrive	Share Point	Total general
jcastaneda_walshp.com.pe#ext#@replica.com.pe	94		94
rborjas_frenosa.com.pe#ext#@replica.com.pe	26		26
urn:spo:anon#10c6f743614d57c5729d277459dcc55a6af81be15ede066d27b1966a8ba183b1	86		86
urn:spo:anon#1db80a49f9cac29b188ef12ae911df3a694716d86011fff1bd2ba41d63825d13	4		4
urn:spo:anon#224fc09a9244611d6924d0262df2ff032b9a38701825b26dea9e98801b4befb9	2		2
urn:spo:anon#2293d2a808ed5a22c846ddc9d662db60b5c72b10b11ea1a3f7041d24193faae2	38		38
urn:spo:anon#4c5db0e6a28a5efccc2b2db787d3578739919b34891ab4cf51f17e8b1f7426f0	5		5
urn:spo:anon#4fcb297c30f19b6cd5d3da0b2ada8ea6de7deb9f6e951b68507ab4ce54d882f7	43		43
urn:spo:anon#601d8716c3a522b293c50a9d62c7c6ba6d4c6f13d8a90318dc379c2fa94addcb	997		997
urn:spo:anon#6993a3d1db31df0ff30f988cc9765c196c2abd94012e4caf940710f5678c3824	2		2
urn:spo:anon#95ea87c91087e74f3677b4fbce9d877988856cfb2be82f9a7a5fe25c235fbcbe	1		1
urn:spo:anon#9a425d605fb13688da0aafdfaccf4152a75937789d7fbb5b771e6de4e8443883	7		7
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	11		11
urn:spo:anon#a7be88d31298265b593806d91be5ecfb82c9a62459dc5aa3a3c55ac6d540cd33	5		5
urn:spo:anon#c6ffdd2ff93ac3b509d59302f03ba6a15ea3ac1ca02eef0c535e9d2164eff7ec	3		3
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93dda5d20bec7b646388	10		10
urn:spo:guest#cloud1@maicolit.com	1		1
urn:spo:guest#jcastaneda@walshp.com.pe	164		164
ventas1@replica.com.pe	18	3	21
ventas2@replica.com.pe	18		18

ventas4@replica.com.pe	11		11
ventas7@replica.com.pe	39		39
user1@replica.com.pe	294	55	349
user3@replica.com.pe	23	195	218
user2@replica.com.pe	9	26	35
user4@replica.com.pe		61	61
user5@replica.com.pe	24	58	82
user6@replica.com.pe	18	21	39
user7@replica.com.pe	29		29
user26@replica.com.pe	4		4
autodesk@replica.com.pe	15	2	17
user21@replica.com.pe	85	14	99
user22@replica.com.pe	3	1	4
user27@replica.com.pe	4		4
user23@replica.com.pe		1	1
user24@replica.com.pe	17		17
user32@replica.com.pe	10		10
user28@replica.com.pe	27		27
user29@replica.com.pe	10	2	12
user31@replica.com.pe	2		2
user25@replica.com.pe	3		3
Total general	2162	439	2601
jcastaneda_walshp.com.pe#ext#@replica.com.pe	94		94
rborjas_frenosa.com.pe#ext#@replica.com.pe	26		26

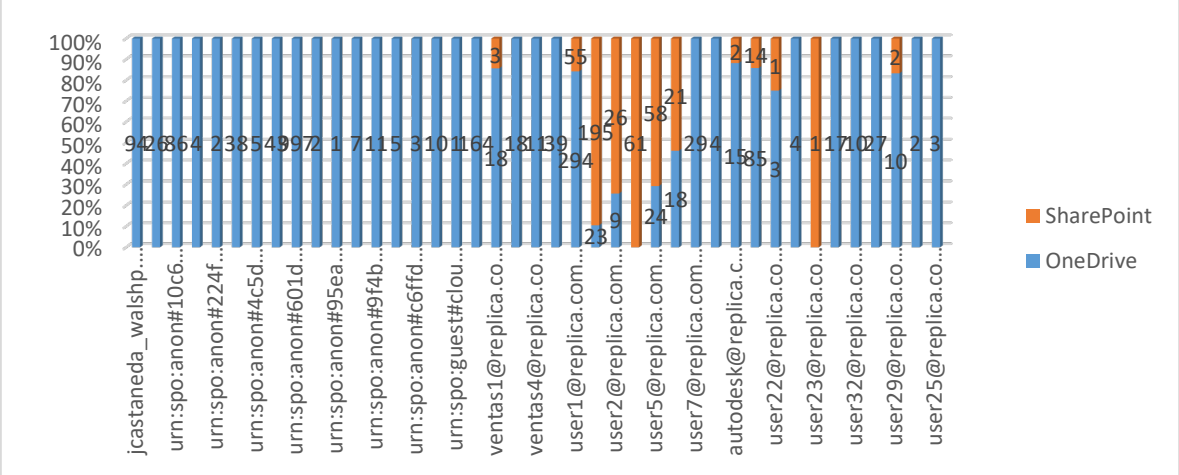


Figura 7. Reporte de Archivos

Fuente: Elaboración propia.

Según el grafico, podemos visualizar que del 100% de usuarios, el 80% pueden ver las descargas o archivos eliminados desde el onedrive, a su vez, estos mismos son usuarios externos e internos que también pueden descargar archivos compartidos. Mientras que el 20%, utilizan el SharePoint.

Tabla 7.

Registro de actividades.

Etiquetas de fila	Cuenta de Operations
urn:spo:anon#601d8716c3a522b293c50a9d62c7c6ba6d4c6f13d8a90318dc379c2fa94addcb	997
user1@replica.com.pe	349
user3@replica.com.pe	218
urn:spo:guest#jcastaneda@walshp.com.pe	164
user21@replica.com.pe	99
jcastaneda_walshp.com.pe#ext#@replica.com.pe	94
urn:spo:anon#10c6f743614d57c5729d277459dcc55a6af81be15ede066d27b1966a8ba183b1	86
user5@replica.com.pe	82
user4@replica.com.pe	61
urn:spo:anon#4fcb297c30f19b6cd5d3da0b2ada8ea6de7deb9f6e951b68507ab4ce54d882f7	43
user6@replica.com.pe	39
ventas7@replica.com.pe	39
urn:spo:anon#2293d2a808ed5a22c846ddc9d662db60b5c72b10b11ea1a3f7041d24193faae2	38
user2@replica.com.pe	35
user7@replica.com.pe	29
user28@replica.com.pe	27
rborjas_frenosa.com.pe#ext#@replica.com.pe	26
ventas1@replica.com.pe	21
ventas2@replica.com.pe	18
user24@replica.com.pe	17
autodesk@replica.com.pe	17
user29@replica.com.pe	12
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	11
ventas4@replica.com.pe	11
user32@replica.com.pe	10
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93dda5d20bec7b646388	7

urn:spo:anon#9a425d605fb13688da0aafdfaccf4152a75937789d7fbb5b771e6de4e8443883	6
urn:spo:anon#4c5db0e6a28a5efccc2b2db787d3578739919b34891ab4cf51f17e8b1f7426f0	5
urn:spo:anon#a7be88d31298265b593806d91be5ecfb82c9a62459dc5aa3a3c55ac6d540cd33	5
user27@replica.com.pe	4
urn:spo:anon#1db80a49f9cac29b188ef12ae911df3a694716d86011fff1bd2ba41d63825d13	4
user26@replica.com.pe	4
user22@replica.com.pe	4
urn:spo:anon#c6ffdd2ff93ac3b509d59302f03ba6a15ea3ac1ca02eef0c535e9d2164eff7ec	3
user25@replica.com.pe	3
user31@replica.com.pe	3
urn:spo:anon#224fc09a9244611d6924d0262df2ff032b9a38701825b26dea9e98801b4befb9	2
urn:spo:anon#6993a3d1db31df0ff30f988cc9765c196c2abd94012e4caf940710f5678c3824	2
user23@replica.com.pe	2
urn:spo:anon#95ea87c91087e74f3677b4fbce9d877988856cfb2be82f9a7a5fe25c235fbcbe	1
urn:spo:guest#cloud1@maicolit.com	1
urn:spo:anon#601d8716c3a522b293c50a9d62c7c6ba6d4c6f13d8a90318dc379c2fa94addcb	1
user1@replica.com.pe	1
Total general	2601

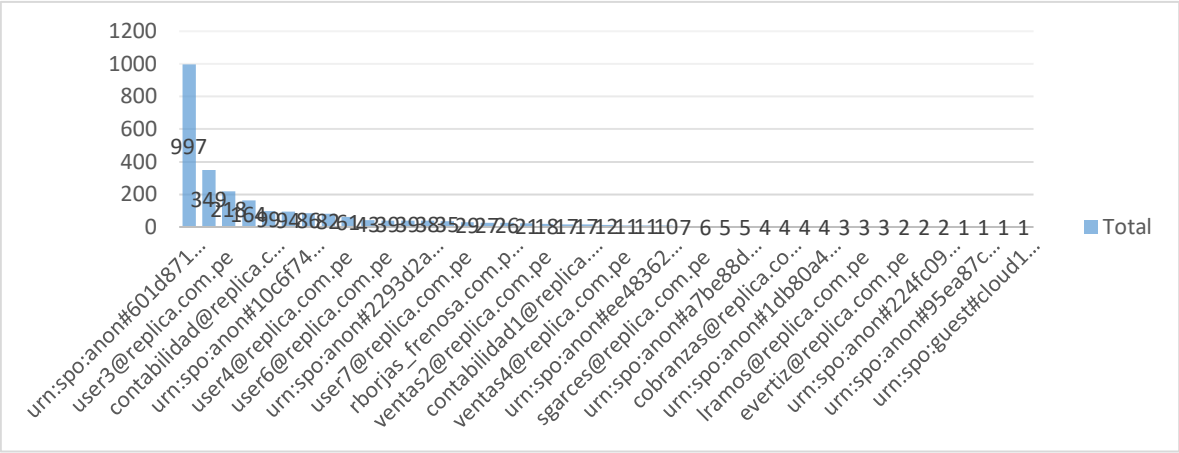


Figura 8. Acciones de SharePoint y OneDrive por usuario.

Fuente: Elaboración propia.

Aquí podemos observar que la mayoría de las acciones se hicieron desde una cuenta anónima o con acceso realizado desde una red externa, cabe mencionar que puede haberse realizado de un dispositivo móvil, celular, tableta y o laptop. Esa cuenta realizo más acciones de descarga y eliminación de archivos.

Tabla 8.

Registro de actividades.

Etiquetas de fila	Cuenta de Operations
OneDrive	2162
SharePoint	439
Total general	**2601**

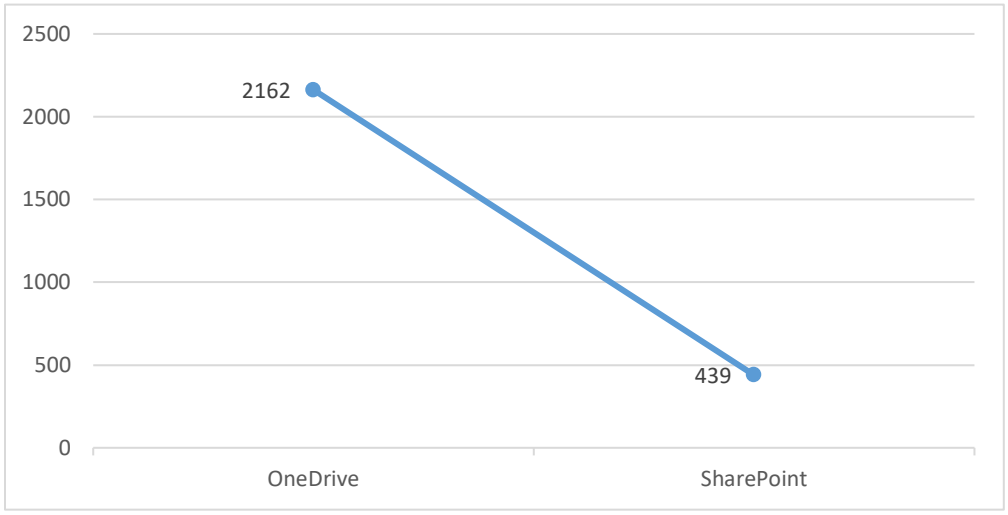


Figura 9. Cantidad de acciones de SharePoint y OneDrive en global.

Fuente: Elaboración propia.

En este grafico visualizamos que la mayor cantidad de archivos con acciones de descarga y eliminados fueren desde el servicio de OneDrive. Mientras que en SharePoint estas acciones son más limitadas, pero siguen siendo data que puede ser sensible para la empresa y debe tener más seguridad y control.

Análisis Cualitativo

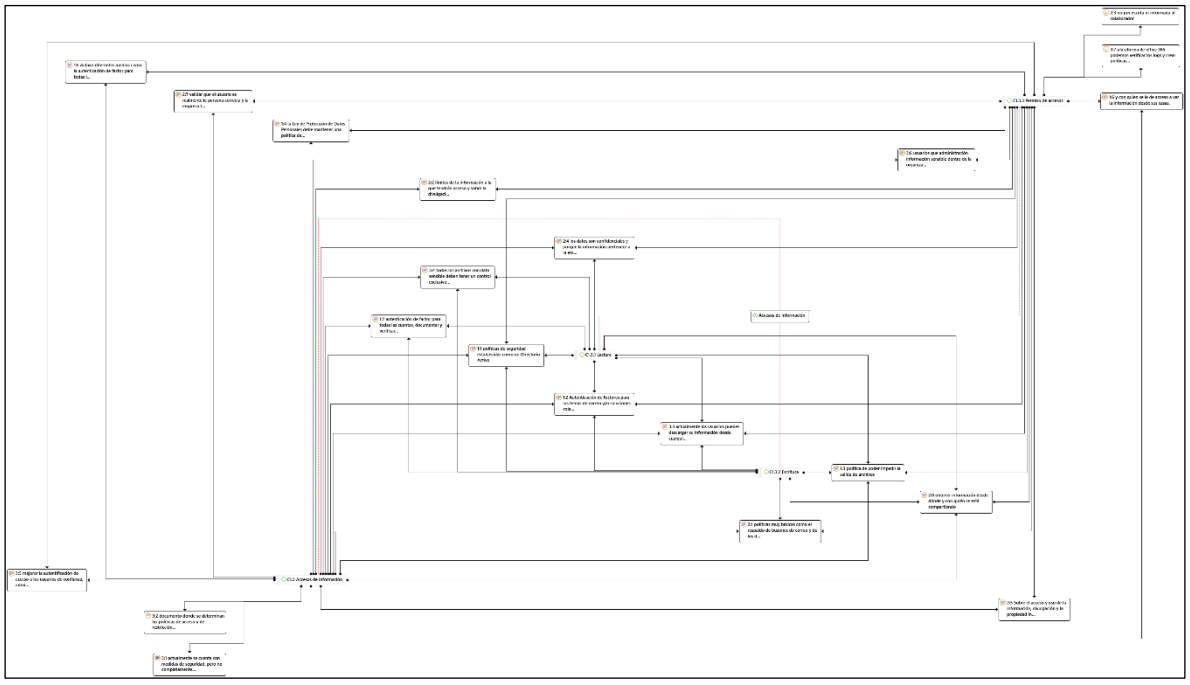


Figura 10. Red de la subcategoría Accesos de información

Fuente: Elaboración propia.

Según la red de la subcategoría de accesos de información que se realizó por medio del análisis cualitativo, podemos identificar que los permisos de acceso a los usuarios no indica las restricciones, por ello no se tiene una política establecida correctamente(falta de comunicación de las políticas de la empresa), de tal modo que se realiza la auditoria de los accesos externos e internos, la descarga de archivos y registro de archivos eliminados desde la plataforma office 365, ya que hay data sensible a la que el usuario podría tener acceso desde su casa y poder descargarla. En este caso, este archivo seria vulnerable ya que no sabremos si cuenta con los requerimientos correspondientes de seguridad para proteger dichos documentos. Se conocen medios diferentes para poder tener la información de la organización con un buen control, pero no se aplica.

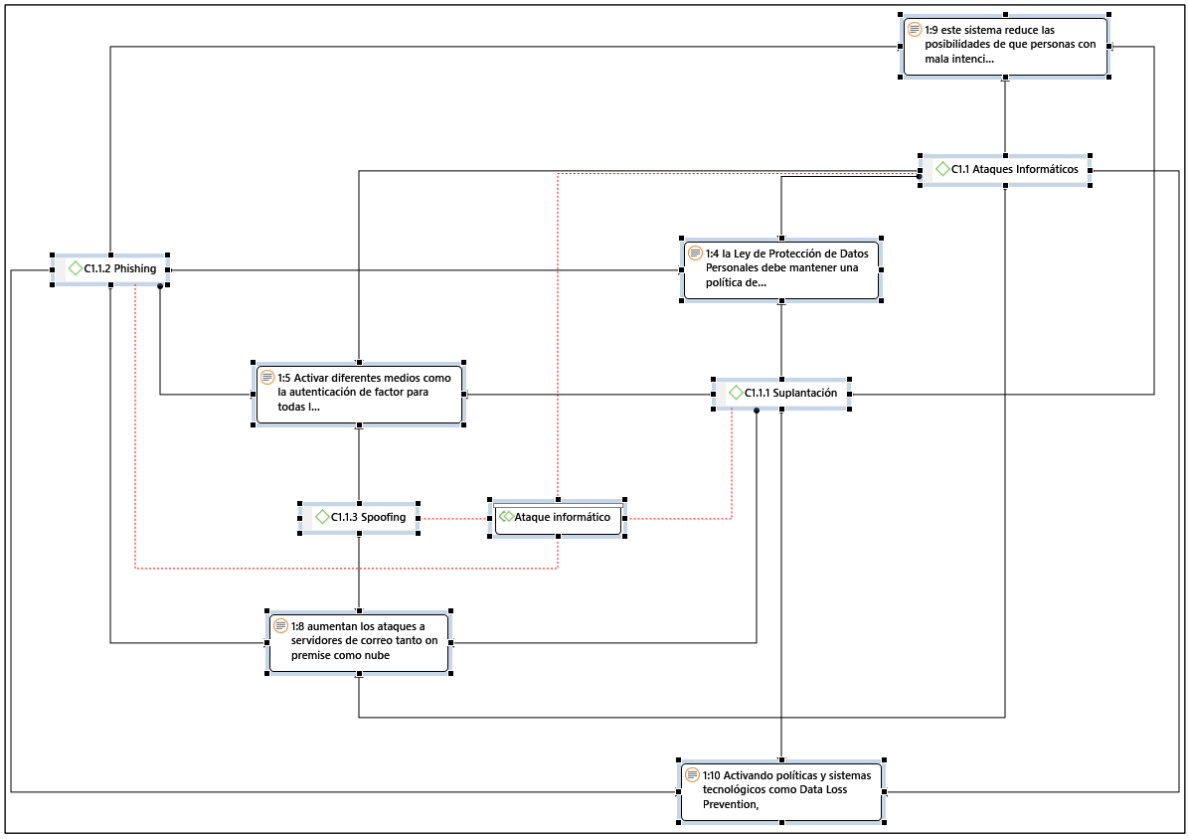


Figura 11. Red de la subcategoría Ataque informático

Fuente: Elaboración propia.

Según la red de la subcategoría de ataque informático que se realizó por medio del análisis cualitativo, verificamos que hay políticas que pueden ayudarnos con la autenticación de los usuarios, y la prevención de perdida de datos, esta categoría nos permite identificar cuáles pueden ser los medios por los que se puede suscitar una pérdida de información, determinando los diferentes tipos de roles y accesos a la información, ya sea de descarga o lectura y escritura de documentos.

Se conocen ataques por correo con contenido mal intencionado, correos con suplantación de identidad o archivos que pueden ser enviados a sus correos personales de cada usuario con información perteneciente a la empresa.

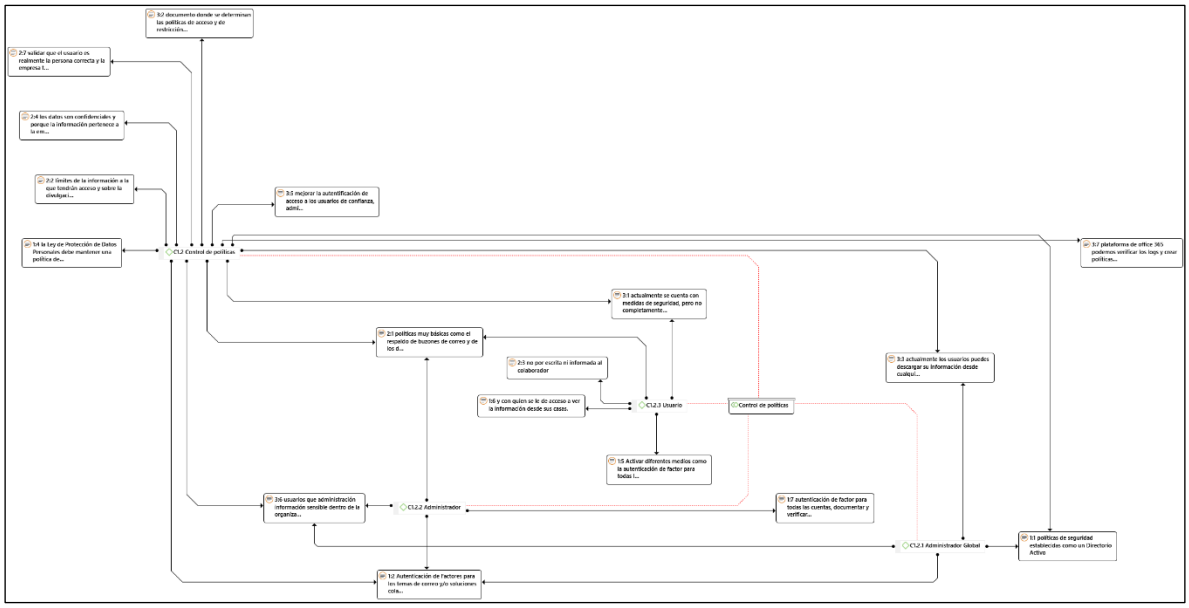


Figura 12. Red de la subcategoría Control de políticas

Fuente: Elaboración propia.

Según el análisis cualitativo tomando como subcategoría el control de políticas se relaciona con los principales roles de administración y de usuarios donde se determinan las políticas de acceso y de restricción que están sustentadas por el administrador global de la plataforma y del directorio activo de la organización, adicional a las políticas se realizan respaldos de buzones y de datos, los usuarios tienen acceso a su información y pueden descargarla cuando configuren su cuenta en sus dispositivos. Al tener en cuenta esta categoría podemos brindar una mejor característica de seguridad implementando las políticas de la plataforma office 365 para el control adecuado de los archivos o data corporativa que no debería ser extraída.

Análisis mixto

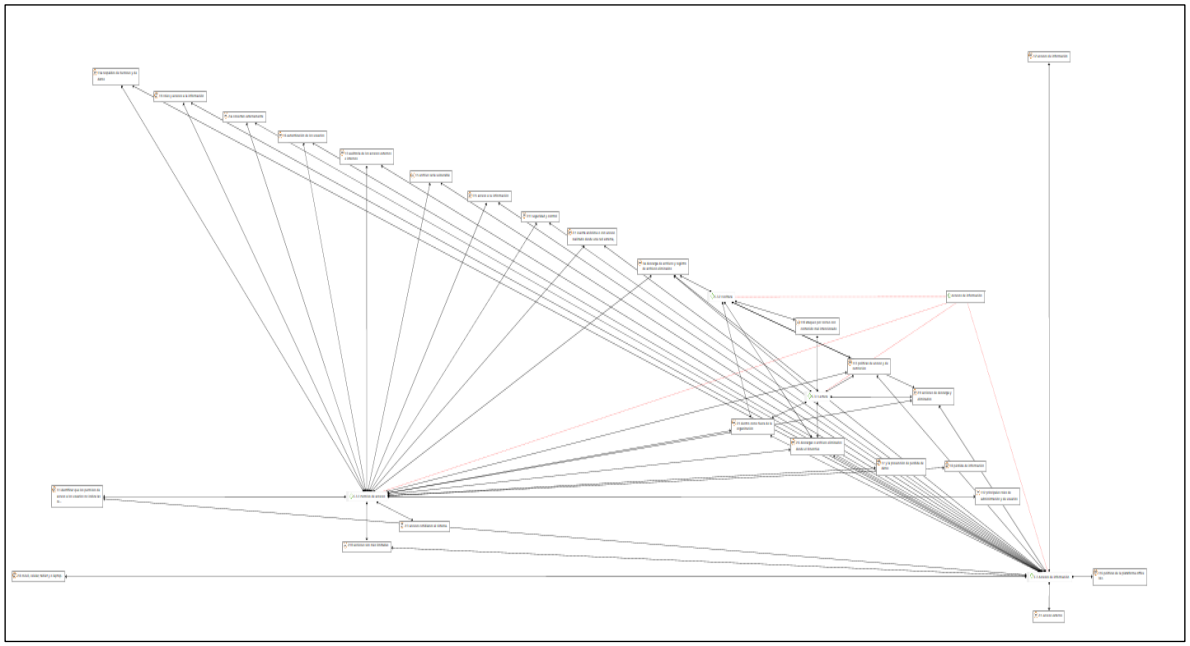


Figura 13. Red de la subcategoría accesos de información

Fuente: Elaboración propia.

Dando uso a la red de triangulación del análisis cualitativo y cuantitativo de la subcategoría accesos de información se obtiene la referencia de que las políticas de accesos y de restricción en documentos por área deben ser implementados, para controlar y prevenir las pérdidas de información, implementando la autenticación multifactor y un pin para cada aplicación que se utiliza para consultar servicios que tengan información a la empresa.

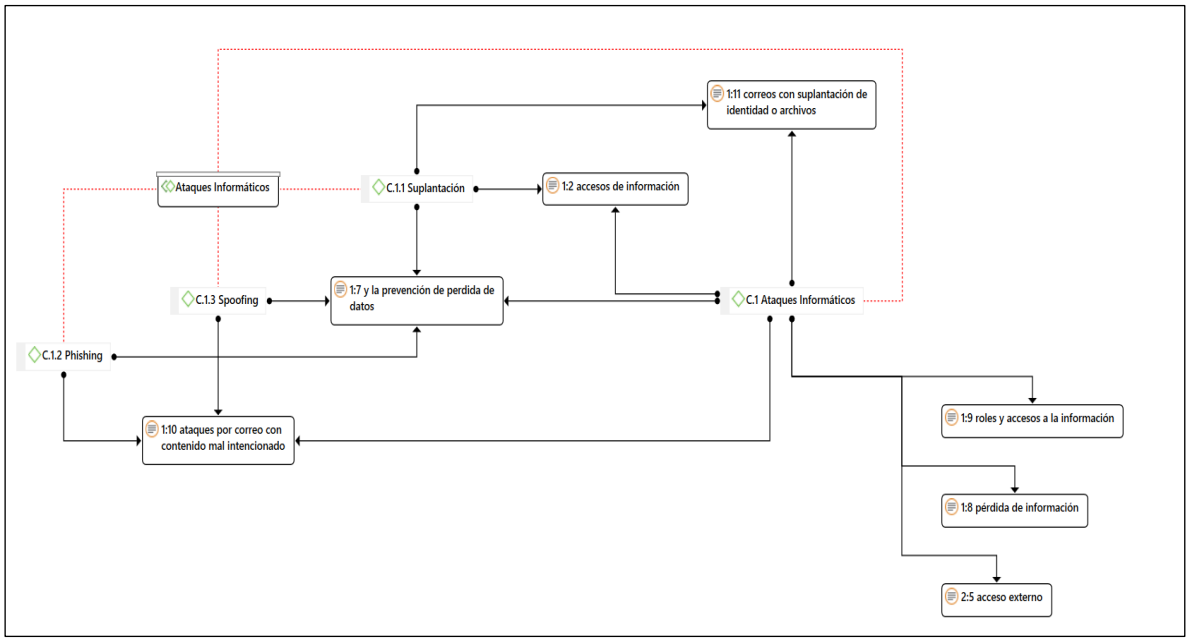


Figura 14.. Red de la subcategoría ataques informáticos

Fuente: Elaboración propia.

En la triangulación de la categoría ataques informáticos y analizando las referencias de los datos recopilados dentro del cuadro cuantitativo y cualitativo, se puede llegar a visualizar la concordancia prevenir ataques informáticos, creando roles para usuarios que acceden desde un lugar externo a la red de la empresa y/o fomentando el uso de sus cuentas en redes externas y o páginas no seguras, de esta manera se evitaría la perdida de datos. De esta manera afirmamos que la empresa necesita implementar estas políticas y configuraciones para la plataforma nube.

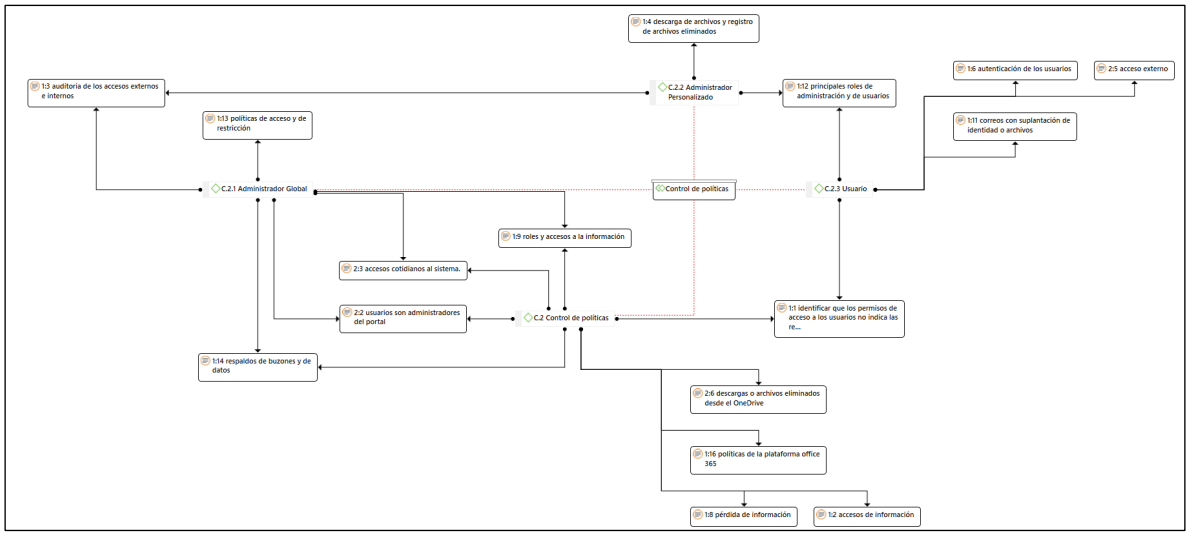


Figura 15. Red de la subcategoría control de políticas

Fuente: Elaboración propia.

En la triangulación de la categoría control de políticas podemos obtener que se tienen tres tipos de rol de usuario donde podemos encontrar al administrador global, administrador personalizado, y usuario, los datos obtenidos indican que los usuarios cuentan con roles básicos de seguridad que pueden permitir la extracción de información relevante para la empresa, se realizan respaldos para evitar data perdida y o fuga de información. Este análisis nos permite identificar que necesitamos las políticas del portal de office 365 activas y correctamente configuradas para poder tener un mejor control en los documentos de la empresa y accesos de los usuarios y mapear a que data ingresan.

4.2 Propuesta

4.2.1 Fundamentos de la propuesta

La propuesta se apoya bajo el fundamento de la teoría general de sistemas, de la cual tomamos sus indicaciones, realizando el trabajo conjunto de los distintos principios, por tal motivo usaremos la conexión de nuestros los tres objetivos determinados para la presente propuesta, que nos permita lograr establecer un sistema complejo que solucione el problema que se plantea, teniendo reconocida la propuesta de solución que plantearemos abajo, y aplicar correctamente la teoría.

De esta misma manera usaremos los fundamentos de la teoría de la información, que nos ayuda a establecer de forma clara como elaborar la data para el usuario y a los administradores después de recopilar la información y el análisis respectivo, que nos ayudara a segmentarlos, ya que sepamos la información sensible de la que los usuarios pueden tener accesos.

Utilizando la teoría general de gestión de riesgo tendremos un mejor conjunto de medidas administrativas, y mejorar nuestras políticas de privacidad, pidiendo reducir el impacto de amenazadas, poder tener el control de cómo controlar una amenaza y reduciendo el ataque por vulnerabilidad

En consecuencia, de esto proponemos realizar una implementación dentro del área de TI, con la claridad y la segmentación correcta para el conocimiento y control de los documentos y dispositivos que deben tener accesos a la información de la empresa Replica S.R.L. que se ubica en Lima, se compromete a apoyar la mejora de para la protección de la información y con la disponibilidad para los usuarios para las capacitaciones correctas teniendo a cambio un mejor resguardo de información.

4.2.2 Problemas

Falta de desarrollo y aplicación de políticas de seguridad, en la plataforma en nube.

Falta de concientización a los colaboradores sobre el uso de la información de la empresa.

Falta de control en los dispositivos móviles de los usuarios.

4.2.3 Elección de la alternativa de solución

	Alternativas de Solución	Evaluación de alternativas: Tiempo 0.10	Costo 0.40	Impacto económico 0.20	Impacto tecnológico 0.10	Impacto social 0.20	✓ 1.00	Puntaje Total	Categoría solución		Problemas	Objetivos de la propuesta
1	S1.- Implementar políticas de seguridad de la información en la plataforma en nube de office 365 en las áreas de la empresa.	4	3	5	5	5		4.100	4.100	S1.- Implementar políticas de seguridad de la información en la plataforma en nube de office 365 en las áreas de la empresa.	A.- Falta de desarrollo y aplicación de políticas de seguridad, en la plataforma en nube.	1.- Implementar políticas de seguridad en la plataforma nube Office 365
2	S2.- Capacitar a los usuarios en políticas de seguridad de la información.	2	2	3	1	3		2.300			B.-Falta de concientización a los colaboradores sobre el uso de la informacion de la empresa.	2.- Concientizar a los usuarios en el uso y las políticas de seguridad de la información.
3	S3.- Implementar y capacitar en políticas de control de dispositivos moviles a los usuarios.	3	3	3	2	3		2.900				
4	S4.-Implementar un administrador de dispositivos moviles para la proteccion de datos corporativos.	4	3	4	4	4		3.600			C.- Falta de control en los dispositivos moviles de los usuarios.	3.- Controlar el acceso a las aplicaciones e información de la empresa desde dispositivos moviles.

Figura 16. Selección de solución.

Fuente: Elaboración propia.

En la siguiente matriz se ingresaron las alternativas de solución de acuerdo con nuestro análisis que de determino con la obtención de los registros de las auditoria por los accesos a las cuentas de correo externas y con equipos celulares y el acceso a la información, descarga de archivos, eliminar archivos sin permiso y sin un control respectivo de la documentación que es extraída.

Según nuestra matriz podemos observar que nuestra categoría solución es implementar políticas de seguridad de la información en la plataforma en nube de office 365 en las áreas de la empresa. Esta implementación a pesar de que nos va a tomar un poco de tiempo asume los puntos correspondientes a las otras posibles soluciones.

4.2.4 Objetivo de la propuesta

Implementar políticas de seguridad en la plataforma nube Office 365.

Concientizar a los usuarios en el uso y las políticas de seguridad de la información.

Controlar el acceso a las aplicaciones e información de la empresa desde dispositivos móviles.

4.2.5 Justificación de la propuesta

En la actualidad se busca plantear una propuesta de implementación que vaya a acuerdo al problema identificado, dentro de la empresa Replica S.R.L. se acepta por el motivo que nos permite reducir el riesgo de pérdida de información y reducir la vulnerabilidad de los archivos sensibles de la empresa.

Por tal motivo la finalidad es delimitar una estrategia que nos permita estructurar la data a la que trabajadores deben tener accesos de lectura, escritura que se configura de la plataforma de office 365 portal de Intune (MDM) para la administración de dispositivos móviles y Azure información protección para los datos sensibles de la empresa, dando por conocimiento de manera documentada e informando a los colaboradores de la empresa: para esto se determinó como fase 1: determinar las políticas a aplicar en los archivos y las áreas que deben tener accesos, como siguiente fase: es concientizar a los usuarios a los cuales se les indicara con capacitaciones como actuar frente a la data sensible de la empresa y como tercera fase: es la configuración de los dispositivos móviles con accesos por PIN para sus aplicaciones que contengan contenido de la empresa, estos deberán ser dispositivos registrados en la plataforma.

4.2.6 Desarrollo de la propuesta

Como primer objetivo: Implementar políticas de seguridad en la plataforma nube Office 365. Como parte del desarrollo se platea una infraestructura desde el análisis de datos, reconocimiento de data sensible y permisos por grupos, áreas y personas. La arquitectura por aplicar será una administración de AIP (Azure Information Protection) y DLP (Data Loss Protection), estos aplicados en el portal de administración en nube, en el que se determina la protección accediendo a OneDrive y SharePoint, permitiendo mantener el control de los documentos pertenecientes a la empresa.

Tabla 9.

Registro de actividades.

ACTIVIDADES:

NRO.	Actividad	Inicio	Días	Fin	Logro parcial	Responsable/s
1	Analizar la información de acceso de los usuarios	1/01/2020	**7**	8/01/2020	Identificar qué tipo de permiso se debe otorgar	Analista 1
2	Analizar la información de los dispositivos más usados en la organización	9/01/2020	**7**	16/01/2020	Mapear desde que dispositivos se tienen más acceso	Analista 1
3	Analizar las políticas que permiten compartir archivos	17/01/2020	**7**	24/01/2020	Identificar qué tipo de archivo son los que salen de la empresa	Analista 1
4	Analizar accesos a la información por áreas de la empresa	25/01/2020	**7**	1/02/2020	Seleccionar la data por áreas	Analista 1 / jefe de proyectos
5	Identificar y etiquetar información sensible	2/02/2020	**4**	6/02/2020	Conocer la data que deberá ser protegida	Analista 1 / jefe de proyectos
6	Implementar control de acceso de los usuarios	7/02/2020	**4**	11/02/2020	Generar la seguridad para la data de la empresa	implementador 1 / jefe de proyectos
7	Implementar políticas para los dispositivos más usados en la organización	12/02/2020	**4**	16/02/2020	Conocer los dispositivos con permisos	implementador 1 / jefe de proyectos
8	Implementar políticas que permiten compartir archivos	17/02/2020	**4**	21/02/2020	Tener data de la empresa segura	implementador 1 / jefe de proyectos
9	Implementar políticas de accesos de la información por áreas de la empresa	22/02/2020	**4**	26/02/2020	Tener orden en documentos	implementador 2 / jefe de proyectos

10	Evaluar políticas implementadas	27/02/2020	**5**	3/03/2020	Conocer la protección actual de la data	Auditor
11	Documentar la implementación de políticas de seguridad de la información	4/03/2020	**3**	7/03/2020	Archivar e informar sobre la protección de la data corporativa	Documentador

Fuente: Elaboración propia.

En esta tabla podemos identificar cuáles son los responsables que necesitamos para cada actividad, que nos ayudara a conocer el tiempo que durara la implementación.

Indicador 1:	**Indicador 2:**
$Log\ auditoria = \frac{Log\ auditoria}{Total\ Log\ de\ auditoria} * 100$	$Politicas\ de\ seguridad = \frac{\#Politicas\ aplicadas}{Total\ de\ politicas\ aplicadas} * 100$

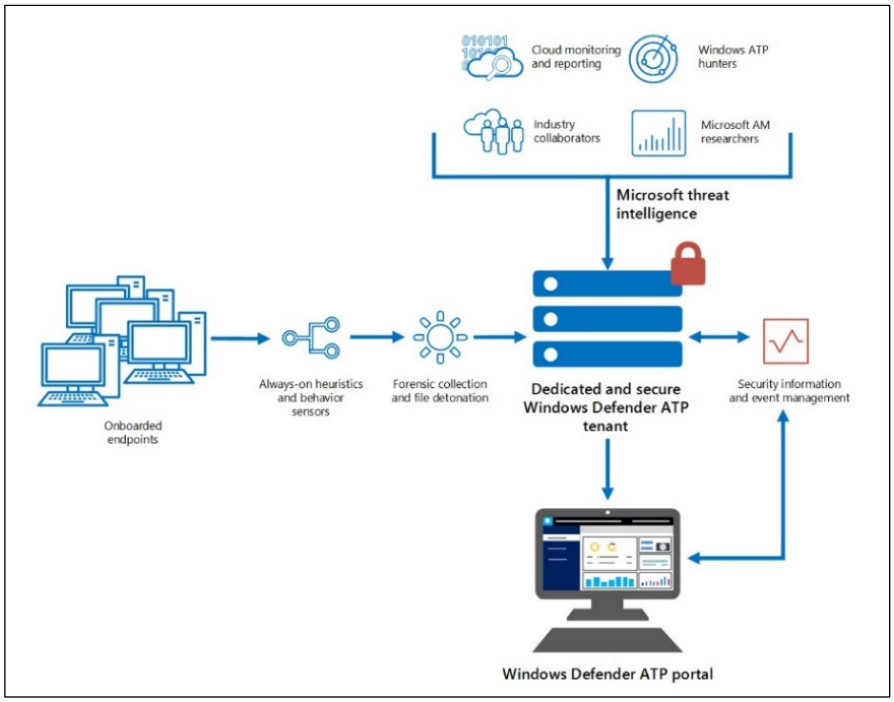


Figura 17. Arquitectura propuesta AIP

Fuente: Microsoft

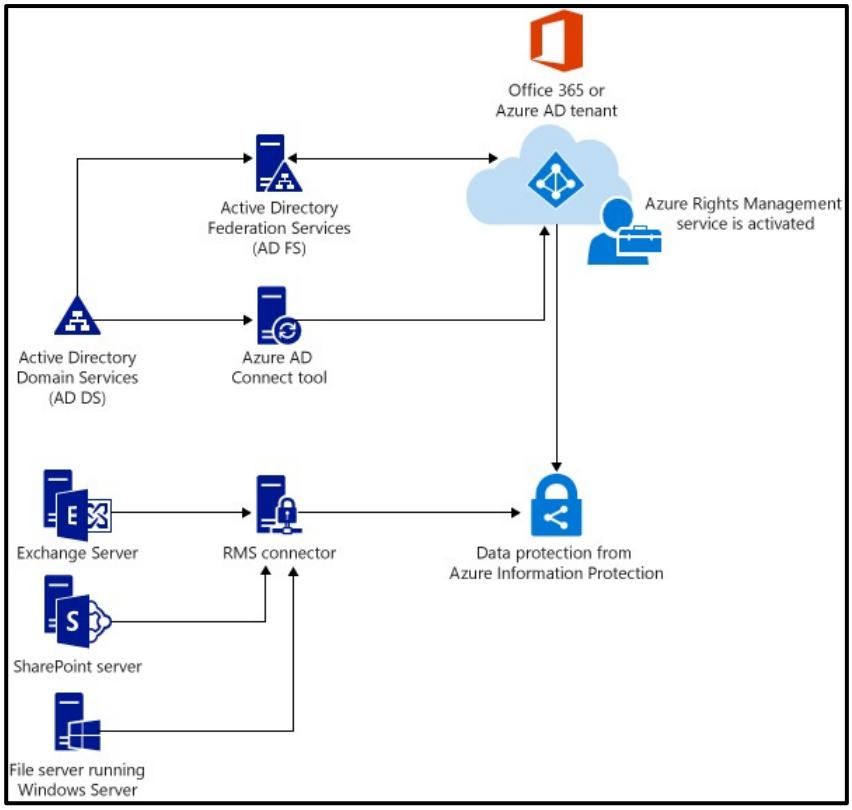


Figura 18. Arquitectura propuesta ARM

Fuente: Microsoft

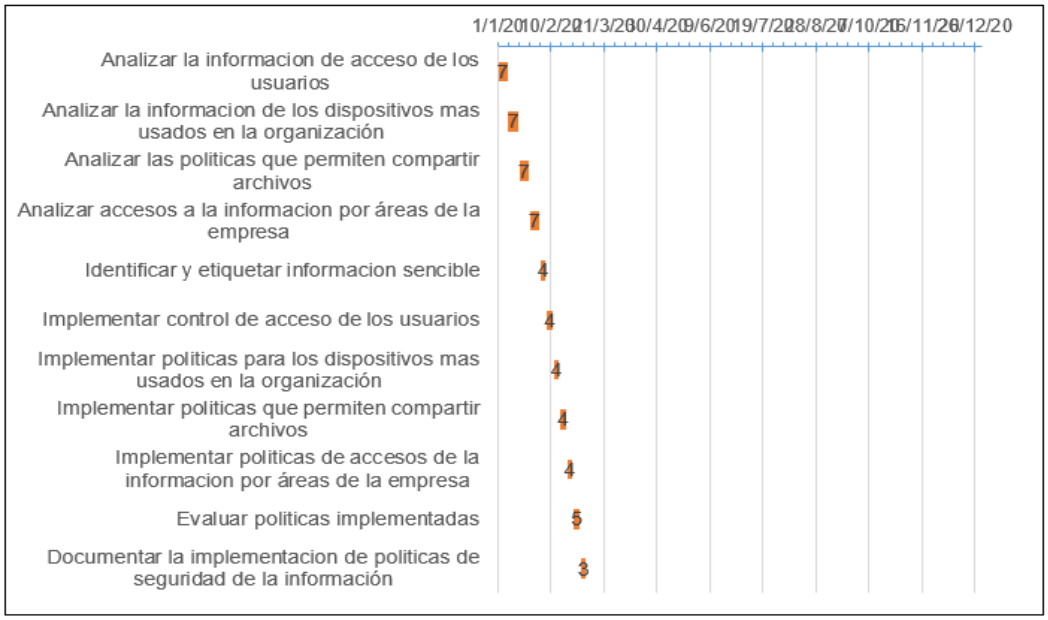


Figura 19. Registro de actividades con tiempos.

Fuente: Elaboración propia.

Se muestra en el siguiente cronograma por fechas y tiempo en el cual terminar el proyecto a implementar, teniendo en cuenta la cantidad de fechas.

Tabla 10.

Registro de actividades de contingencia.

Actividad	Justificación
Analizar la información de acceso de los usuarios	Revisar los permisos para el análisis de los accesos de cada usuario
Analizar la información de los dispositivos más usados en la organización	Consultar a cada usuario los dispositivos desde los que tiene accesos a la data de la empresa
Analizar las políticas que permiten compartir archivos	Revisar los archivos compartidos o enviados
Analizar accesos a la información por áreas de la empresa	Consultar que usuarios tienen acceso a la información de la empresa
Identificar y etiquetar información sensible	Consultar que archivos deberían ser protegidos
Implementar control de acceso de los usuarios	Informar que usuarios necesitan accesos controlado
Implementar políticas para los dispositivos más usados en la organización	Informar sobre el control de los dispositivos de la empresa
Implementar políticas que permiten compartir archivos	Informar que archivos deben tener permiso para ser compartidos
Implementar políticas de accesos de la información por áreas de la empresa	Informa los roles de los usuarios en las diferentes áreas de la empresa
Evaluar políticas implementadas	Revisar las políticas implementadas y su funcionamiento
Documentar la implementación de políticas de seguridad de la información	Informar cambios que necesitan ser documentados

Fuente: Elaboración propia.

En este cuadro se visualiza las opciones a tomar como plan de contingencia en cada una de las actividades para poder cumplir con el objetivo planteado y culminar con la implementación en el tiempo propuesto.

Para iniciar con nuestra configuración como primera actividad se analizará la información de acceso de los usuarios, esto se refiere desde que dispositivos acceden a sus

cuentas y cuáles son los usuarios con más accesos en fines de semana o días laborales, revisando el acceso es solo para la plataforma de correo o incluye el centro documental.

Como siguiente objetivo analizaremos la información de los dispositivos más usados en la organización, podremos segmentar por áreas los permisos que deben tener y las aplicaciones confiables que puedan descargar.

En esta actividad será apoyado por un analista que revisara políticas deben estar permitidas por usuarios para compartir archivos.

En este paso deben trabajar el analista y el jefe de proyectos analizando accesos a la información por áreas de la empresa. Se debe tener una buena segmentación para que la información no caiga en manos equivocadas.

En este paso el analista debe identificar y etiquetar información sensible para poder separar y crear una política aparte, para los usuarios que tengan acceso a esta data.

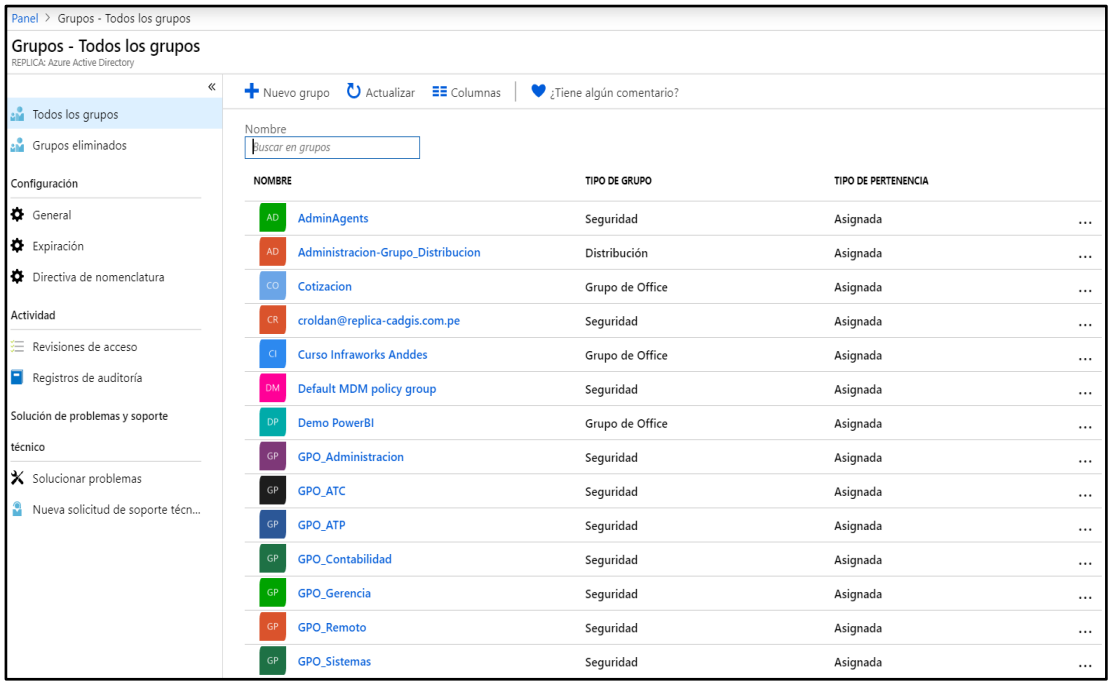


Figura 20. Portal Active Directory Azure

Fuente: Microsoft

En esta actividad el Implementador generara los controles de acceso para los usuarios.

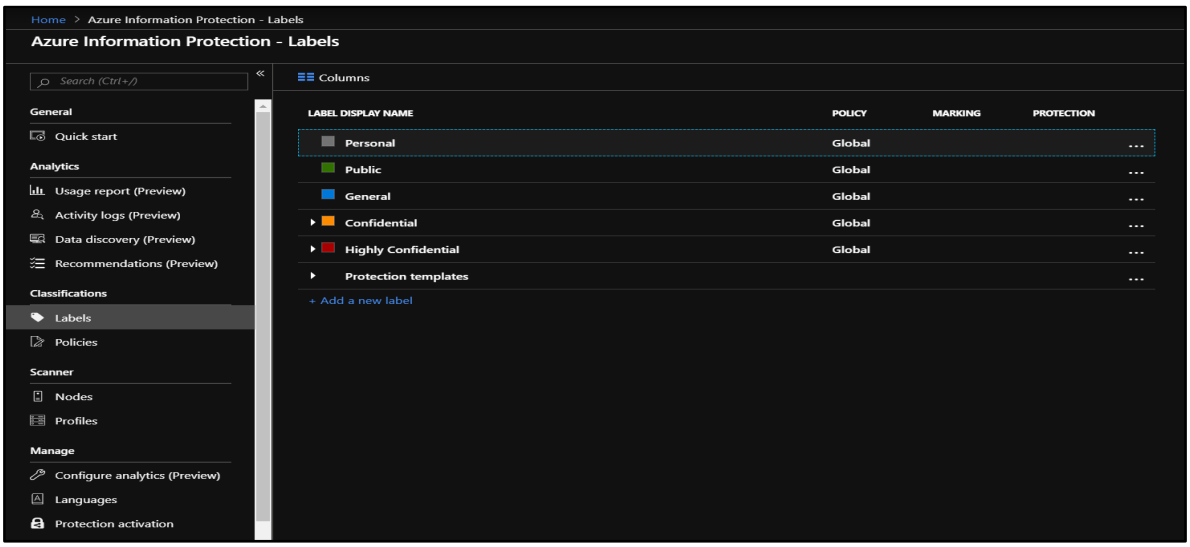


Figura 21. Portal Azure Information Proteccion

Fuente: Microsoft

El implementador realizara las configuraciones de cada política determinada para los dispositivos más usados en la organización.

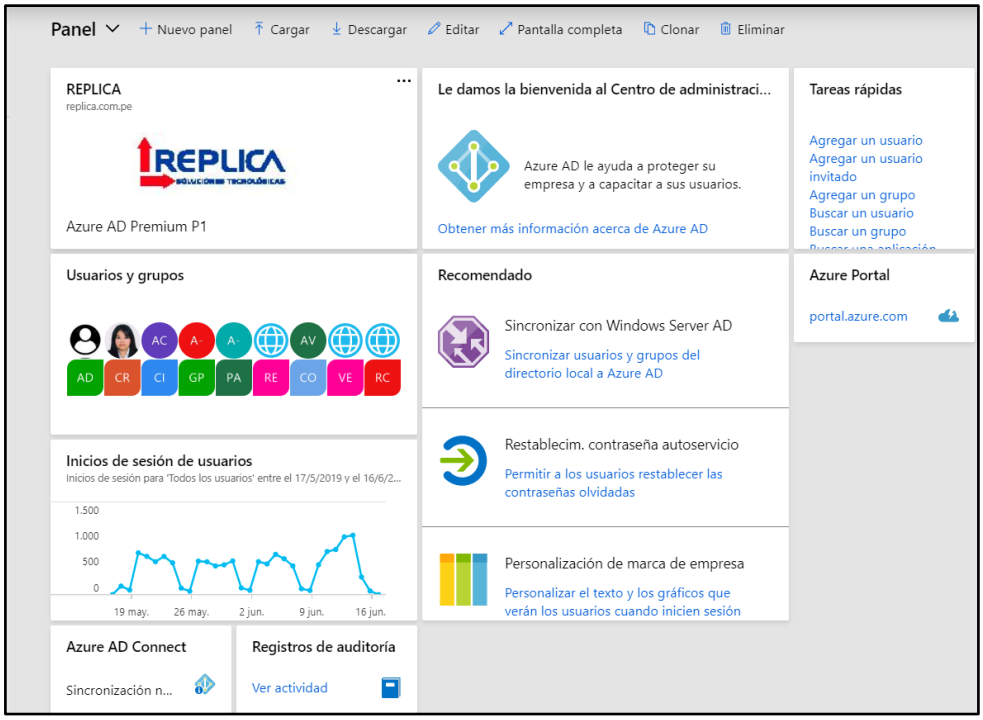


Figura 22. Portal de Intune

Fuente: Microsoft

El implementador realizará las configuraciones e implementar políticas para los grupos de archivos a los que se tendrá acceso y podrán compartir.

El implementador genera las políticas de accesos de la información por áreas de la empresa, esto nos permitirá, controlar los ingresos y salidas de información.

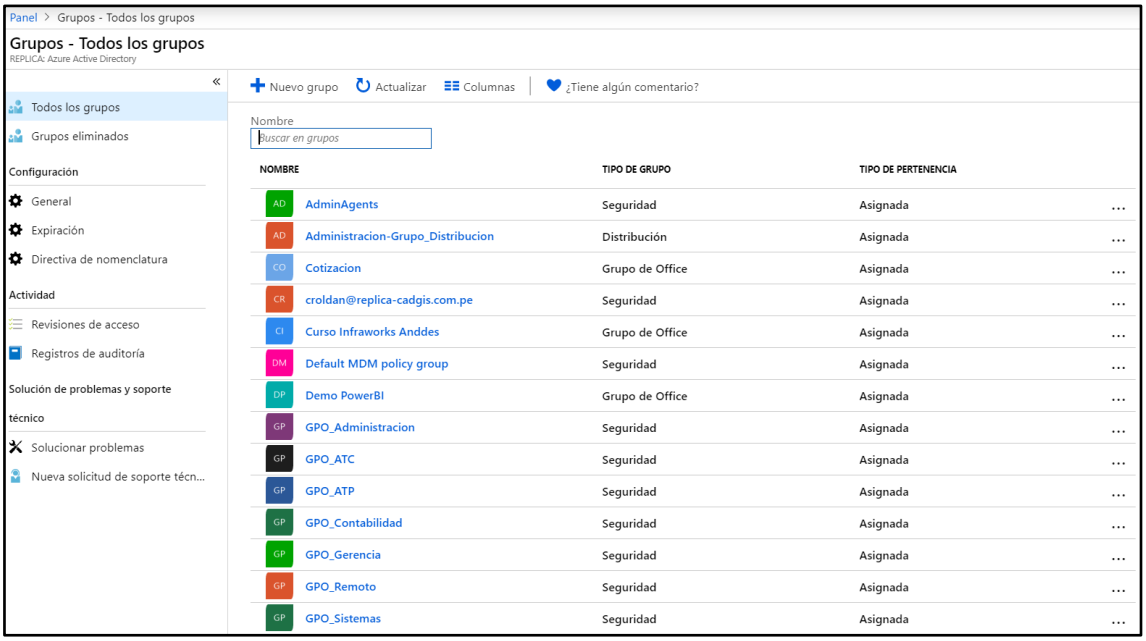


Figura 23. Plataforma de grupos

Fuente: Microsoft

El auditor se presentará para evaluar que se cumplan con las normas para hacer válidas las políticas implementadas.

El documentador generara los informes y registros de los hechos para la implementación de políticas de seguridad de la información utilizando la plataforma MDM de Intune y Azure Protección de la información.

Como segundo objetivo: Controlar el acceso a las aplicaciones e información de la empresa desde dispositivos móviles. Como parte del desarrollo de la propuesta se plantea una infraestructura desde la administración de dispositivos. La arquitectura para aplicar será un básico MDM que consiste en un agente en nuestro caso será portal empresa de office 365, se

instala la aplicación en los dispositivos que se deben administrar, un servidor de en plataforma nube nos ayudara con la configuración necesaria por dispositivo y una base de datos donde se almacén todas las configuraciones realizadas. Los agentes mantienen una conexión con el servidor a través de USB, Wi-Fi, GPRS, 3G o diferentes medios de transmisión de datos, lo cual le permite al MDM tomar control del dispositivo, en sus algunos casos cubriendo características de lista de aplicaciones no deseadas, el control remoto de la solución y arreglo de los problemas en las máquinas alejadas, podría ser reseteo y o eliminación de cuenta, administración de la información que este dentro del dispositivo perteneciente a la empresa, gestión de contenido, actualizaciones de OS.

Tabla 11.

Registro de actividades.

Actividad	Inicio		Fin	Logro parcial	Responsable/s
Revisar, asignar, validar tipo de licencia en el portal	1/01/2020	1	2/01/2020	Reconocer el tipo de licencias que se tienen activas	Jefe de proyectos / Administrador
Distribuir a los usuarios por áreas	3/01/2020	1	4/01/2020	Segmentar la lista por áreas	Analista / jefe de proyectos
Activar y configurar el multifactor de autenticación	5/01/2020	1	6/01/2020	Permisos activados para la configuración	Implementador
Habilitar el portal de Intune para dispositivos Android	7/01/2020	1	8/01/2020	Configurar para Android	Implementador
Habilitar el portal de Intune para dispositivos iPhone	9/01/2020	1	10/01/2020	Configurar para IPhone	Implementador
Habilitar el portal de Intune para dispositivos Windows	11/01/2020	1	12/01/2020	Configurar para Windows	Implementador
Crear políticas de acceso y seguridad para dispositivos Android	13/01/2020	1	14/01/2020	Crear permisos para Android	Implementador
Crear políticas de acceso y seguridad para dispositivos iPhone	15/01/2020	1	16/01/2020	Crear permisos para IPhone	Implementador

Crear políticas de acceso y seguridad para dispositivos Windows	17/01/2020	5	22/01/2020	Crear permisos para Windows	Implementador
Configurar políticas de control de dispositivos	23/01/2020	1	24/01/2020	Dispositivos configurados	Implementador
Implementar etiquetas de información sensible	25/01/2020	4	29/01/2020	Segmentar documentación	Implementador
Evaluación de políticas implementadas	30/01/2020	5	4/02/2020		Auditor / jefe de proyectos

Fuente: Elaboración propia.

Indicador 1:

$$Dispositivos = \frac{Dispositivos\ no\ registrados}{Total\ de\ dispositivos} * 100$$

Se necesita revisar, asignar, validar el tipo de licencia en el portal ya que con el conocimiento de los tipos de licencia podremos saber que políticas podemos aplicar.

Distribuir a los usuarios por áreas

Activar y configurar el multifactor de autenticación

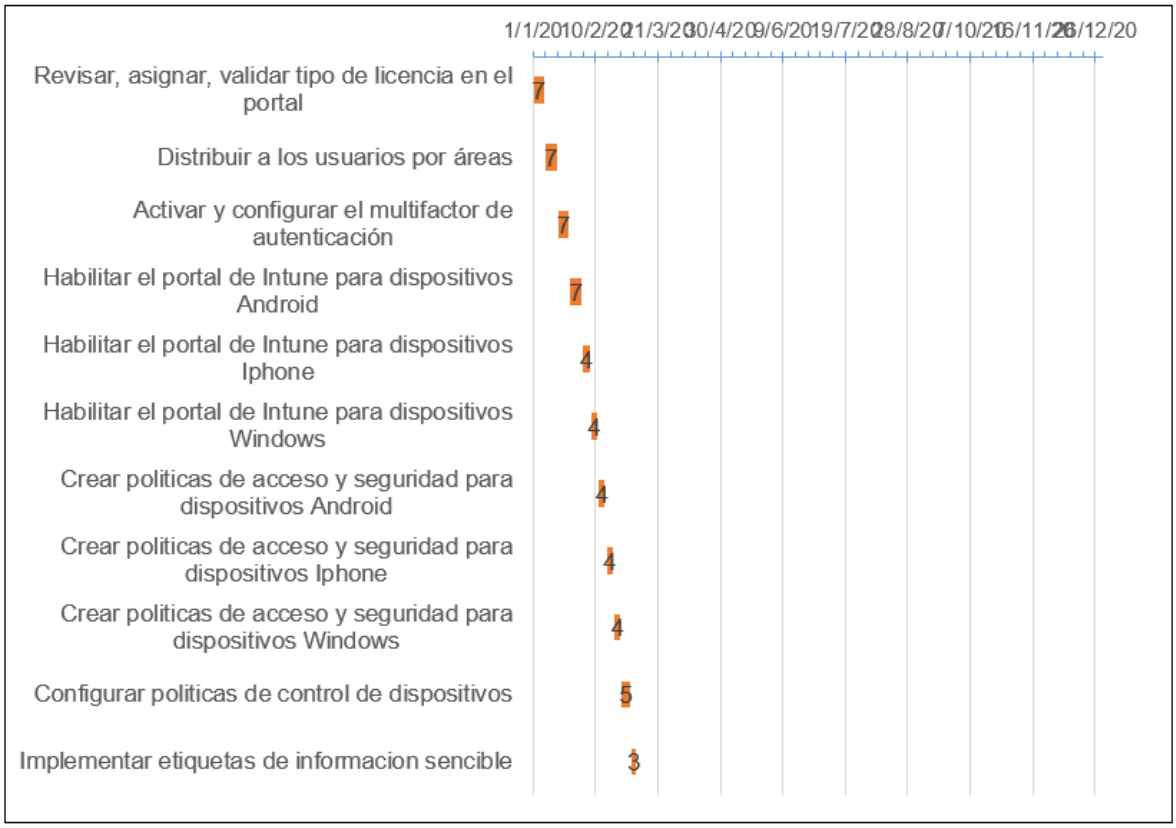


Figura 24. Registro de actividades con tiempos.

Fuente: Elaboración propia.

Se muestra en el siguiente cronograma por fechas y tiempo en el cual terminar el proyecto a implementar, teniendo en cuenta la cantidad de fechas.

Se necesita revisar, asignar, validar el tipo de licencia en el portal ya que con el conocimiento de los tipos de licencia podremos saber que políticas podemos aplicar.

Distribuir a los usuarios por áreas

Activar y configurar el multifactor de autenticación

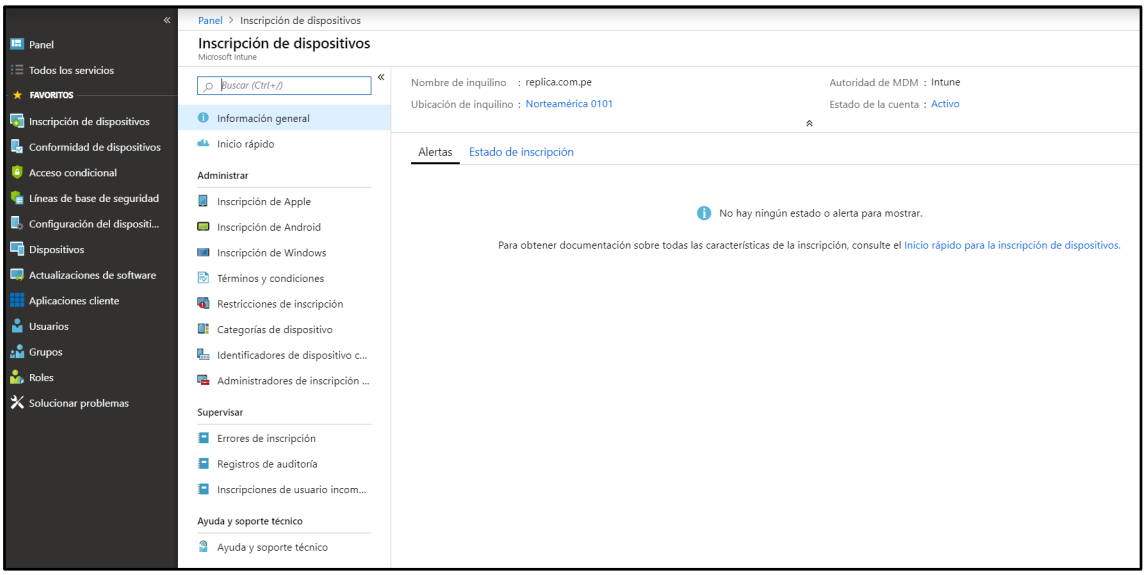


Figura 25. Registro de Dispositivo

Fuente: Microsoft

Habilitar el portal de Intune para dispositivos Android, IPhone, Windows esto nos permitirá poder activar las características que necesitan ser cumplidas, para el manejo de la información de la empresa en estos dispositivos.

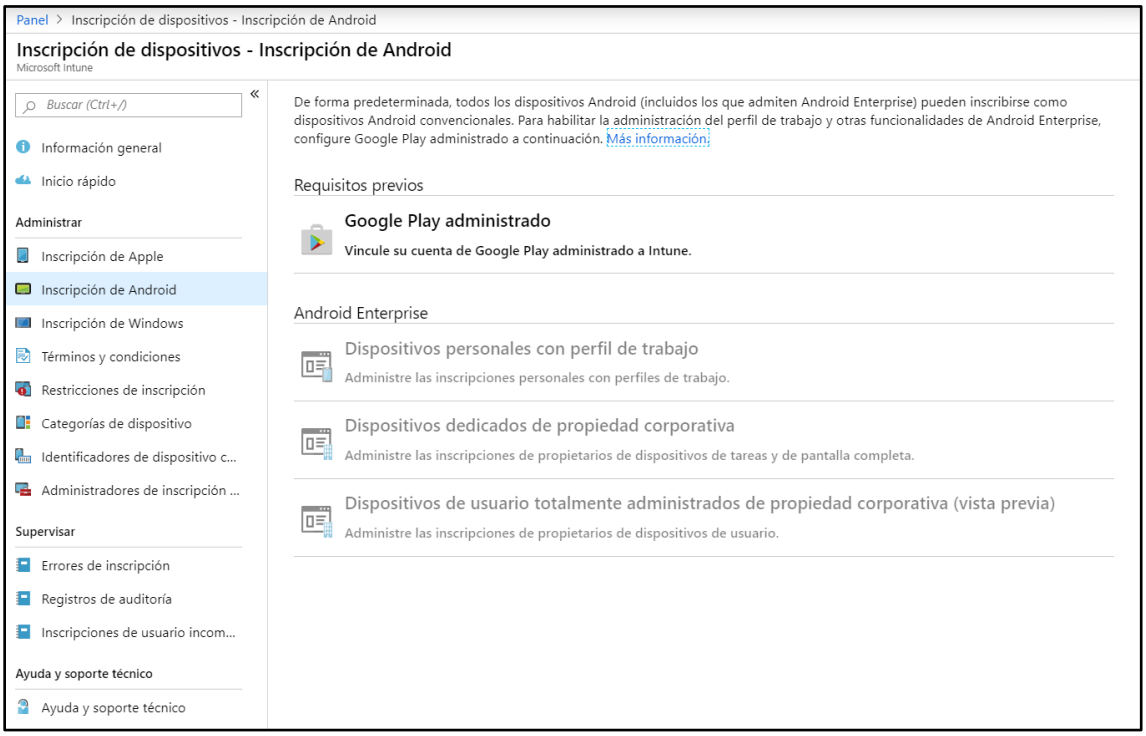


Figura 26. Registro de Dispositivo para Android

Fuente: Microsoft

Crear políticas de acceso y seguridad para dispositivos Android, IPhone y Windows los cuales nos facilitaran el control de la data y los dispositivos, por seguridad de sustracción o perdida del equipo.

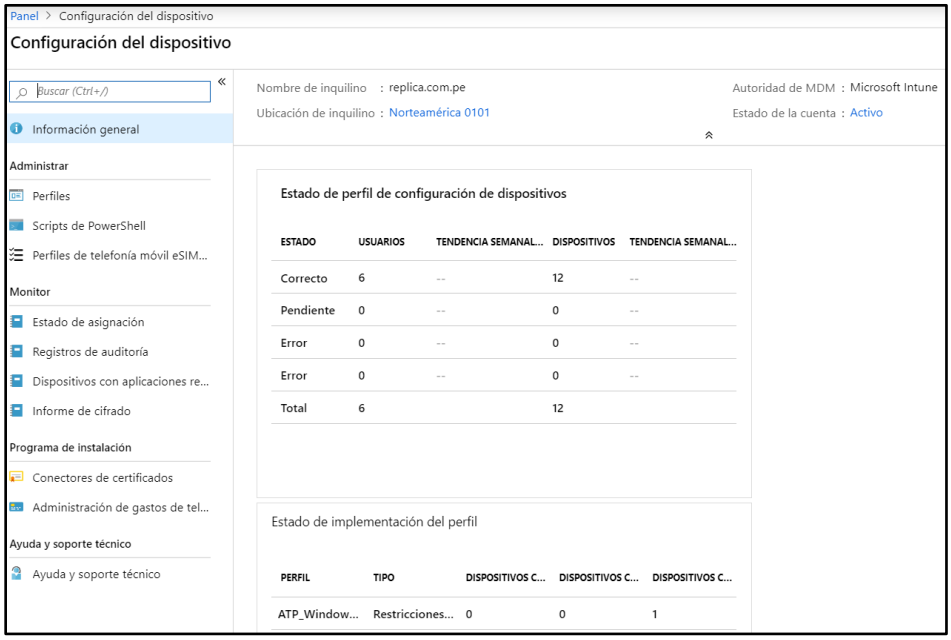


Figura 27. Configuración de políticas

Fuente: Microsoft

Configurar políticas de control de dispositivos

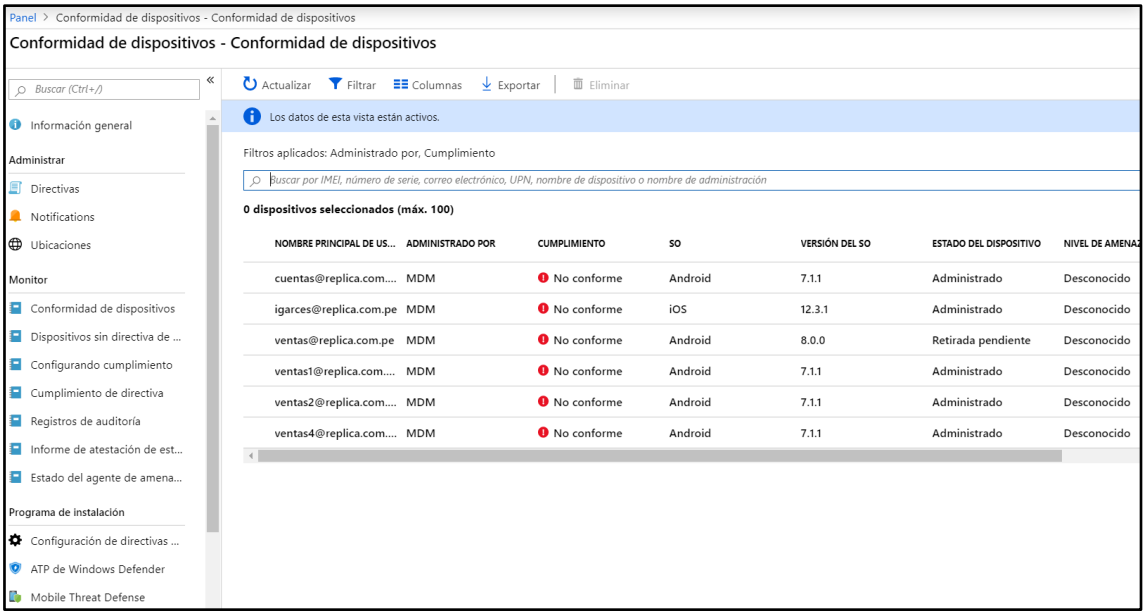


Figura 28. Revisando conformidad con los dispositivos y cuentas

Fuente: Microsoft

Implementar etiquetas de información sensible, evaluar políticas implementadas

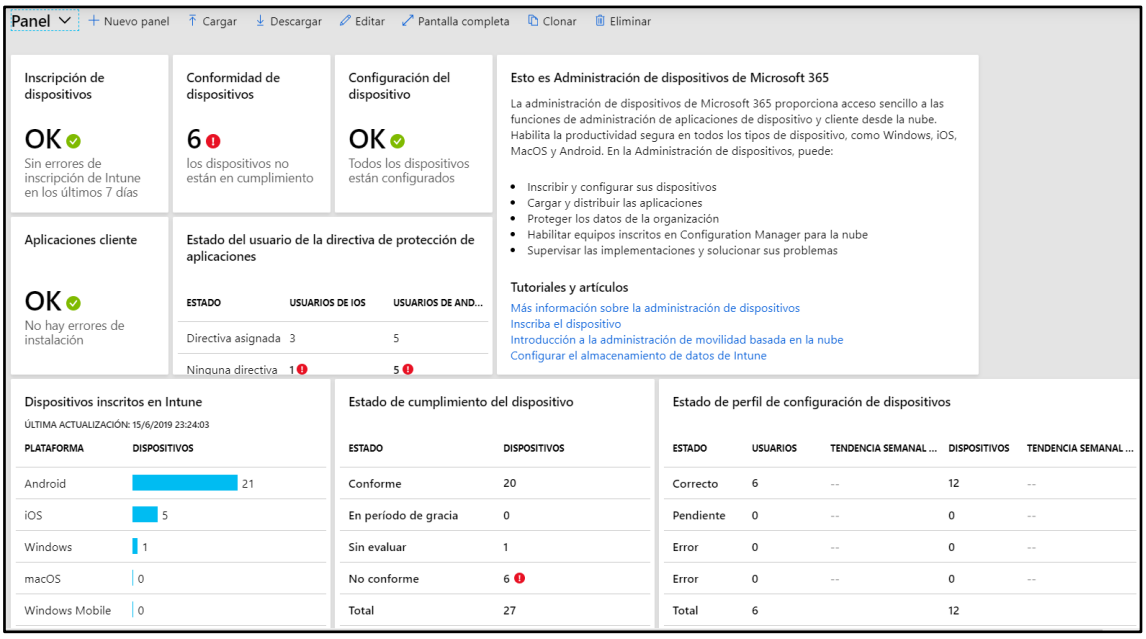


Figura 29. Portal de reporte

Fuente: Microsoft

Tabla 12.

Registro de actividades de contingencia.

Revisar, asignar, validar tipo de licencia en el portal	Solicitar permisos al administrador
Distribuir a los usuarios por áreas	Solicitar información de usuarios por área
Activar y configurar el multifactor de autenticación	Solicitar permiso para acceder a dicha información
Habilitar el portal de Intune para dispositivos Android	Solicitar permisos para administrar portal
Habilitar el portal de Intune para dispositivos IPhone	Solicitar permisos para administrar portal
Habilitar el portal de Intune para dispositivos Windows	Solicitar permisos para administrar portal
Crear políticas de acceso y seguridad para dispositivos Android	Informar sobre los beneficios de la aplicación de las políticas
Crear políticas de acceso y seguridad para dispositivos IPhone	Informar sobre los beneficios de la aplicación de las políticas
Crear políticas de acceso y seguridad para dispositivos Windows	Informar sobre los beneficios de la aplicación de las políticas
Configurar políticas de control de dispositivos	Solicitar permisos para la configuración

Implementar etiquetas de información sensible	Crear informe de data sensible

Fuente: Elaboración propia.

Se evalúan medidas de contingencia que se puedan utilizar en caso se encuentre alguna complicación para las actividades determinadas

Como tercer objetivo: Concientizar a los usuarios en el uso y las políticas de seguridad de la información. Como parte del desarrollo de la propuesta se plantea que los usuarios deben estar familiarizados con las actuales mejoras que se llevaran a cabo para la protección de los datos de la empresa, se deberá capacitarlos y orientarlos en el uso de la autenticación por usuario y cómo será el manejo de la data a la que tengan acceso fuera de la empresa.

Tabla 13.

Registro de actividades.

Actividad	Inicio	Días	Fin	Logro parcial	Responsable/s
Generar grupos por área	1/01/2020	1	2/01/2020	Agrupar a los usuarios para la capacitación	Administrador / jefe de proyectos
Preparar presentación	3/01/2020	2	5/01/2020	Tener un mejor control de la explicación	Capacitador
Preparar las herramientas para transmitir la información	6/01/2020	3	9/01/2020	Dar una guía sobre el tema	Documentador
Capacitación para el área de ventas	10/01/2020	1	11/01/2020	Área de Ventas capacitada	Capacitador / jefe de proyectos
Capacitación para el área de facturación	12/01/2020	1	13/01/2020	Área de facturación capacitada	Capacitador / jefe de proyectos
Capacitación para el área de ATP	14/01/2020	1	15/01/2020	Área de ATP capacitada	Capacitador / jefe de proyectos
Redactar encuestar	16/01/2020	1	17/01/2020	Medir la información recibida	Documentador

Fuente: Elaboración propia.

Se puede observar el cuadro de participantes involucrados en la realización de este primer objetivo, los cargos que tendrán los participantes y los tiempos que se tomarán para la realización del objetivo.

Figura 30. Registro de actividades con tiempos.

Fuente: Elaboración propia.

Se muestra en el siguiente cronograma por fechas y tiempo en el cual terminar el proyecto a implementar, teniendo en cuenta la cantidad de fechas.

Tabla 14.

Registro de actividades de contingencia.

Actividad	Justificación
Generar grupos por área	Solicitar tiempo a los usuarios
Preparar presentación	Adquirir información relevante a los usuarios
Preparar las herramientas para transmitir la información	Revisar artículos con información para los usuarios
Capacitación para el área de ventas	Dirigirse a cada usuario para explicarle los cambios
Capacitación para el área de facturación	Dirigirse a cada usuario para explicarle los cambios
Capacitación para el área de ATP	Dirigirse a cada usuario para explicarle los cambios
Redactar encuestar	Consultar a cada usuario su experiencia

Fuente: Elaboración propia.

Indicador 1:

$$Acceso\ de\ información = \frac{\#Ususarios\ con\ acceso}{Total\ de\ información\ usada\ en\ dispositivos\ móviles} * 100$$

En este indicador podremos obtener que usuarios frecuentemente utilizan los dispositivos móviles en los cuales se incluyen laptops, ya que los usuarios de ventas asisten a reuniones y tienen accesos desde esos dispositivos.

Indicador 2:

$$Usuarios\ concientizados = \frac{Usuarios\ no\ concientizados}{Total\ de\ usuarios\ no\ concientizados} * 100$$

En este objetivo incluimos a los usuarios, generando grupos para la capacitación, de entregarán manuales, de crearán herramientas demostrativas las cuales podrán ser de apoyo hasta su adopción correcta en el caso del autenticador multifactor se indicará la función de las políticas de seguridad implementadas, realizando una encuesta, para medir el aprendizaje de estos.

4.3 Discusión

La presente investigación titulada "Implementación de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en la empresa Replica S.R.L. 2019", se propuso como objetivo proponer políticas de seguridad de la información para proteger la data sensible que utilizan en la empresa Replica.

Utilizamos dos técnicas que se emplearon para recopilar datos la cual fue la recolección de datos y ficha de entrevista permitieron obtener un diagnostico concreto a su vez estos datos nos permiten analizar los registros de auditoria y comprender que usuarios utilizan información de la empresa fuera de la red IP asignada, para esta evaluación se consideró a todos los usuarios dentro del portal en nube del que se administran las licencias, y a tres Jefes

de las áreas informáticas por sus respuestas en las entrevistas realizadas. En nuestro diagnostico cuantitativo.

En el diagnostico cuantitativo la subcategoría accesos de información fue la principal de la categoría siendo el 80% de problemas de la empresa comercial Replica, según el resultado obtenido podemos responder la interrogante del problema general teniendo en cuenta la información de los entrevistados y los logs de auditoria.

La empresa comercial Replica requiere la solución planteada la cual consta de la activación de políticas de seguridad de la información, autenticando la información de cada usuario al registrarse en un nuevo equipo, segmentar la información a la que se debe tener acceso.

Determinar la data sensible, la cual se avala con Alcántara (2015) que coincide con el objetivo de contribuir en la mejora del nivel de seguridad de la información. Empleando las políticas de seguridad de la información que se configuran en la plataforma en nube, la cual se segmentara por grupos desde Azure AD.

Realizando estas configuraciones podremos tener relación con el objetivo del estudio de Bermúdez y Bailón (2015) de los cuales su objetivo fue analizar los procesos críticos para respaldar la confidencialidad, integridad y disponibilidad de la información, ya que cada usuario puede tener accesos para una mejor productividad, con relación al estudio de Vasquez (2015), se determinó la prevención de los ataques cibernéticos, para esto tendremos un mejor control por usuario.

Para evaluar las mejoras, se capacitará a los usuarios referente a las políticas implementadas, realizando encuestas se obtendrá los datos de la mejoría, realizaremos la documentación correspondiente a las políticas aplicadas.

CAPÍTULO V

CONCLUSIONES Y SUGERENCIAS

5.1 Conclusiones

Primero: Se propuso la implementación de políticas de seguridad para proteger la información corporativa de tal manera reducir y evitar la salida de datos corporativos y mantener un control de los documentos.

Segundo: Se basó el diagnostico en un estudio cuantitativo y cualitativo que se trabajó de la mano con la ayuda con el administrador de Sistemas para la obtención del log de auditoria del cual obtuvimos resultados indicando que la mayoría de los accesos a cuentas era de manera externa.

Tercero: Se trabajó con categorías, subcategorías e indicadores los cuales se pudo conceptualizar con la ayuda de artículos y tesis encontrados, así mismo nos ayudó a conocer más sobre el tema de investigación percibir que son enriquecedores para poder generar un a propuesta de implementación.

Cuarto: Se planteó una implementación de las políticas de seguridad para mejorar el control de acceso a la data de la empresa, reduciendo así la posibilidad de ataques con el autenticador de usuarios y utilizando un token, para cuando se genere un intento de acceso a data de la empresa, agregando portal de administración para el control de los dispositivos con acceso a la data de la empresa.

5.2 Sugerencias

Primero: Establecer la propuesta en el área correspondiente, nos permita implementar, el control correcto para los accesos de las cuentas y archivos de la empresa, teniendo en cuenta la disposición de esta y el cumplimiento que nos permita tener seguir manteniendo la productividad.

Segundo: Conocer las ventajas de la protección de los datos nos permitirá reducir el riesgo de la perdida de información, o modificación de documentos a los cuales no se debería de acceder.

Tercero: Se debe actualizar constantemente en la configuración de las políticas del portal en nube, ya que este cambia constantemente, relacionarse con las características más amplias y mejorar la protección.

Cuarto: Para una mejor administración en dispositivos celulares se recomienda utilizar los dispositivos móviles de Samsung y IPhone ya que traen desde fabrica un sistema de protección de datos que se relaciona con el portal en nube y esto nos permite tener un mejor control de dicho dispositivo.

CAPÍTULO VI

REFERENCIAS

Bibliografía

Abreu, J. L. (2014). El Método de la Investigación. *Daena: International Journal of Good Conscience*, 195-204.

Aetecno. (31 de julio de 2018). Aetecno. *americaeconomia*, 1-2. Obtenido de Aetecno.

Albarracín, J. (2002). La teoría del riesgo y el manejo del concepto riesgo en las sociedades agropecuarias andinas. *CIDES-UMSA, Posgrado en Ciencias del Desarrollo*, 1-27.

Areitio Bertolín, J. (2008). *Seguridad de la información, redes, informática y sistemas de información.* Madrid: Paraninfo.

Baca Urbina , G. (2016). *Inttroducción a la Seguridad informática.* Mexico: Patria.

Báez, J., & Pérez, T. (2009). *Investigación cualitativa.* Madrid: Editorial ESIC.

Benavides, C. (2016). *Auditoría financiera a las cuentas caja y bancos de la empresa distribuidora de alimentos S.A.S. de conformidad con NIAS.* contador: Bucaramanga: Universidad cooperativa de colombia.

Benito Jaén, A. (1981). *Fundamentos de teoría general de la información.* Madrid: Editorial Piramide.

Bertalanffy, L. (1989). *Teoría general de Sistema.* Distrito Federal: Fondo de cultura económica.

Capurro, R. (2007). Epistemología y ciencia de la información. *Revista Venezolana de Información, Tecnología y Conocimiento*, 11-29.

Cärdenas Barrios, L. (2016). La Herramienta Informática Atlas ti En el Análisis de Fuentes Históricas de las Prácticas Educativas del Siglo XIX. *Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática*, 265-269.

Chicano Tejeda, E. (2014). *Gestión de incidentes de seguridad informatica. IFCT0109.* Málaga: IC Editorial.

Chuquisengo, O., Pinedo, L., Torres, A., & Rengifo, F. (2005). Guía metodológica para la gestion de riesgos de desastres en los centros de educación primaria. *ITDG*, 1-148.

Corral, Y. (2010). Diseño de cuestionarios para recoleccion de datos. *Ciencias de la educación*, 152-168.

Días Rivel, F., & Rosales Ortiz, R. (2003). *Los resultados de la evaluación.* Costa Rica: Univercidad Nacional a Distancia.

Fermín, F. (2012). La Teoría de Control y la Gestión Autónoma de Servidores Web. *COMTEL 2012*, 73-78.

Fernández, L. (2007). Fichas para investigadores. *Butlletí LaRecerca*, 1-9.

Fernández-Pinto, I., López-Pérez,, B., & María, M. (2008). Empatía: Medidas, teorías y aplicaciones en revisión. *Universidad de Murcia*, 284.298.

Gutierrez, J. (2003). *Protocolos criptográficos y seguridad en redes.* Santander: Univercidad de Cantabria.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodologia de la investigación.* Mexico: Interamericana Editores, S.A.

Hurtado de Barrera, J. (2000). *Metodologia de la investigacion holistica.* Caracas: Servicios y proyecciones para America Latina.

Israel, D. (junio de 2016). *Itsitio*. Obtenido de Itsitio: https://www.itsitio.com/ec/todos-los-caminos-llevan-a-la-nube/

Jaime Gutiérrez, J. (2003). *Protocolos criptográficos y seguridad en redes.* Obtenido de https://books.google.com.pe/books?id=cQk_Ms6MUfEC&pg=PA14&dq=proteccion+de+la+informacion&hl=es&sa=X&ved=0ahUKEwiunuK4i-riAhVJK7kGHYlbA3IQ6AEIOjAD#v=onepage&q=proteccion%20de%20la%20informacion&f=false

Lopez, A., Parada, A., & Simonetti, F. (1995). *Teoria de la información.* Santiago.

López, N., & Sandoval, I. (2013). *Métodos y técnicas de investigación cuantitativa y cualitativa.* Guadalajara.

Marqués, S. D. (2017). Cómo usar Authenticator, app para gestionar la verificación en dos pasos en todas las redes. *Trecebits*, 1.

Núñez Vidal, E., Villarroel González, C., & Cuevas Gil, V. (2010). *Suplantación de la identidad.* Universidad Complutense de Madrid.

Ojeda, C. (2017). *SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO.* Magdalena. Obtenido de http://www.infotephvg.edu.co/cienaga/hermesoft/portalIG/home_1/recursos/julio_2017/05072017/manual-sst.pdf

Parra Moreno, D. A. (2012). *Gestión de riesgo en la seguridad informatica: Cultura de la auto-seguridad informática.* Especialización en Control Interno: Bogota: Universidad Militar Nueva Granada.

Rayme Serrano, R. (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades : un estudio de tres casos en Lima Metropolitana.* Lima: Universidad Nacional Mayor de San Marcos.

Revista Cleu. (2013). La suplantación de identidad. *Colectivo Arcion*, 7-21.

Ruiz Larraguivel, E. (1990). *Propuesta de un modelo de evaluacion curricular para el nivel superior.* Mexico: Univercidad Autonoma de Mexico.

Sainz-Aloy, A., & Soy-Aumatell, C. (2011). Gestión eficiente del correo electrónico: una experiencia corporativa. *Criteria CaixaCorp SA*, 571-576.

Sarabia, A. (1995). *La teoria general de Sistemas.* Madrid: Editorial Isdefe.

Sistema de Gestión Integrado. (2017). Gestion de Logs y registros de auditoría. *Superintendencia de sociedades*, 1-7.

Tamayo, A. (1998). *Sistemas de Información.* Colombia: Universidad Nacional de Colombia.

UCM. (2019). *Ingeniería de Sistemas y de Control.* Madrid: Universidad complutense.

Valbuena, F. (1997). *Fundamentos de teoría general de la información.* Madrid: Universidad Complutense.

Zanabria, J. G., Sánchez Aguilar, A., & Montoya Sánchez, L. (Mayo de 2019). *informe Tecnico Producto Nacional.* Lima: Producción Nacional. Obtenido de informe Tecnico Producto Nacional.

ANEXOS

Anexo 1: Matriz de la investigación

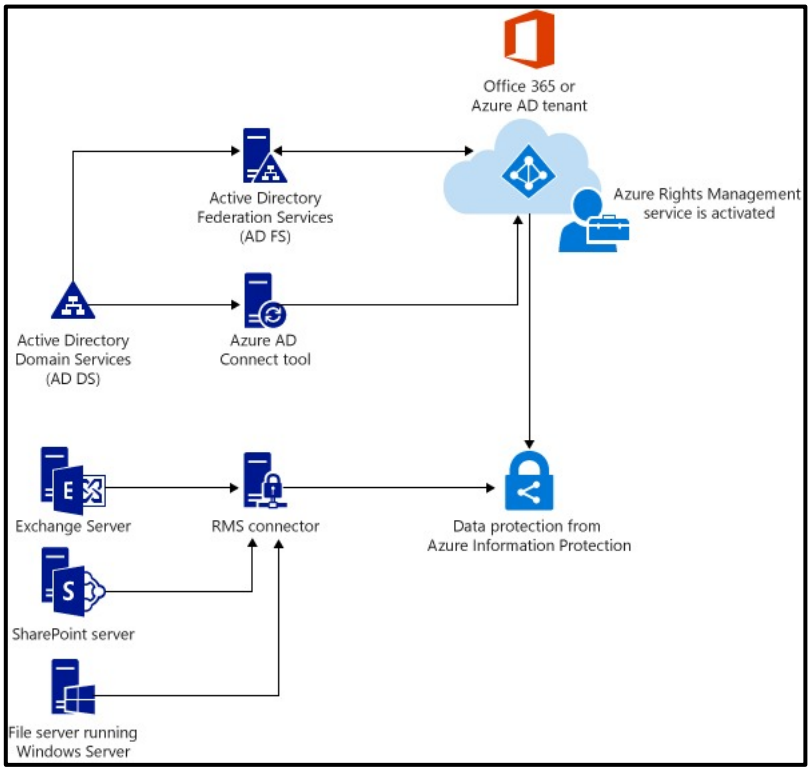
Problema general	**Objetivo general**	**Hipótesis general**	**Categoría 1:**				
			Sub categorías	**Indicadores**	**Item**	**Escala**	**Nivel**
¿Cómo aumentar la protección de la información en la empresa Replica dentro de la plataforma de Office 365 de sus usuarios?	Proponer políticas de seguridad de la información que utilizan en la empresa Replica.	Las políticas de seguridad protegerán con un 70% la documentación de la empresa Replica SRL.	Confidencialidad	1. Falta de Seguridad en el uso de sus contraseñas			
				2. Faltan de restricciones en la compartición de la información			
			Disponibilidad	3. Restricciones de acceso desde redes públicas de los empleados			
				4. Permisos asignados a los empleados para su uso particular			
			Licenciamiento	5. Falta de conocimientos de los administradores de la plataforma Office 365 de la empresa Replica			
				6. Falta de aplicación de las licencias adquiridas para la seguridad de la plataforma de Office 365			
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**	**Categoría 2:**				
			Sub categorías	**Indicadores**	**Item**	**Escala**	**Nivel**
¿Cómo es la protección de la información en la empresa Replica?	Analizar las políticas de seguridad en la empresa Replica S.R.L.			1.			
¿Cuáles son los factores/causas de mayor	Explicar las causas de mayor demanda la seguridad de la			2.			
				3.			

inseguridad en la empresa replica?	información en la empresa Replica.			4.			
¿Como las estrategias influyen en la seguridad de la información?	Predecir la influencia de las políticas de seguridad en la empresa Replica.			5.			
				6.			

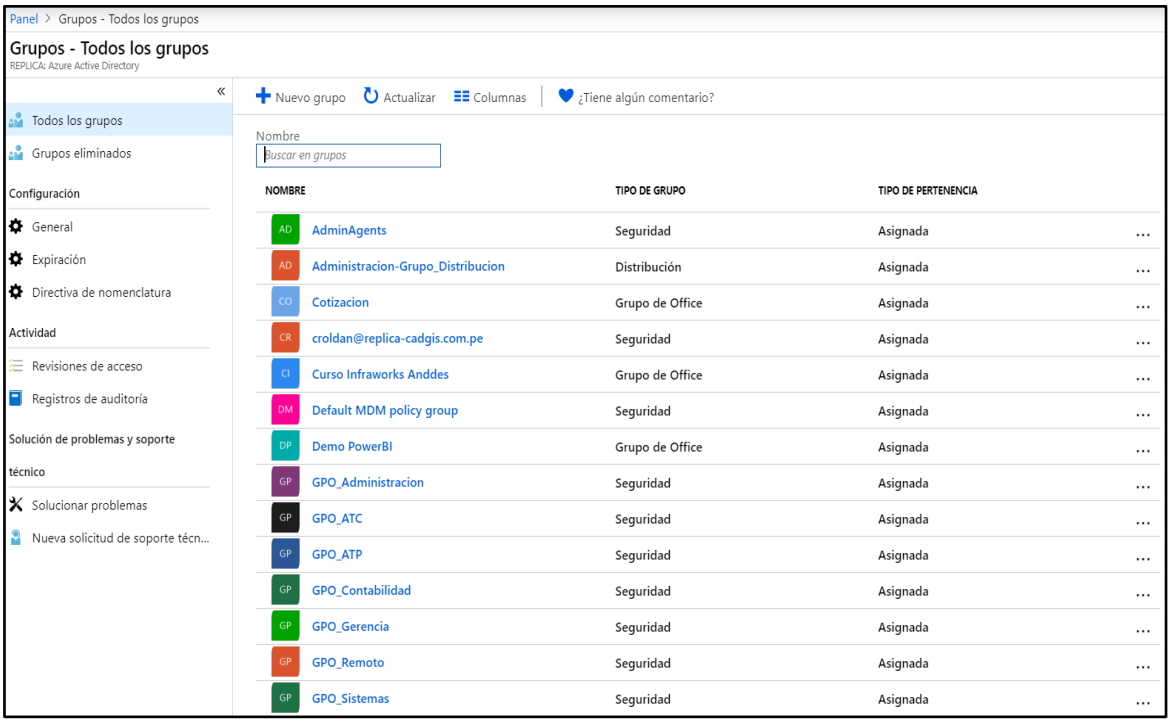
Tipo, nivel y método	**Población, muestra y unidad informante**	**Técnicas e instrumentos**	**Procedimiento y análisis de datos**
Sintagma: Holístico Tipo: Proyectiva Nivel: Comprensivo Método: Deductivo e inductivo	Población: 30 Colaboradores Muestra: Replica Unidad informante: Área de sistemas, ATP.	Técnicas: T. cuantitativa Encuesta T. Cualitativa Entrevista Instrumentos	Procedimiento: Análisis de datos: Regresión medida de frecuencia, Porcentaje de Pareto.

Anexo 2: Evidencias de la propuesta

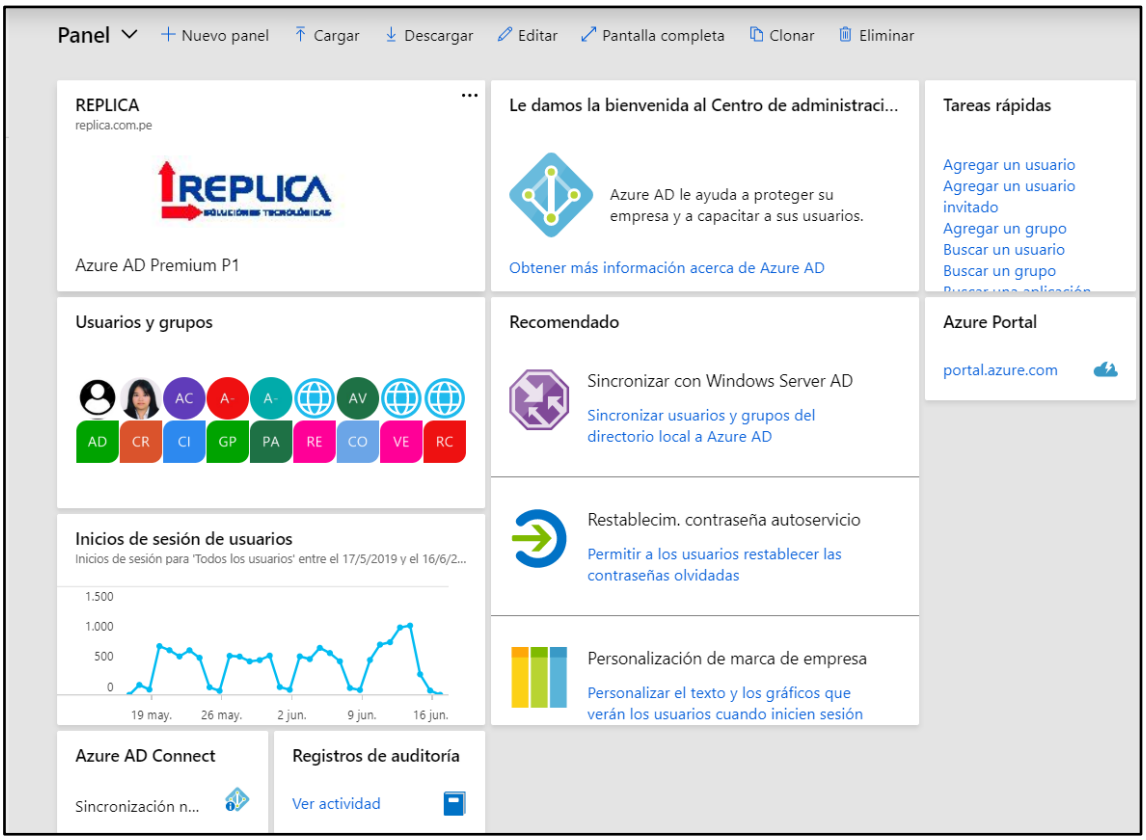
Diagrama de funcionamiento de Azure Information Protection



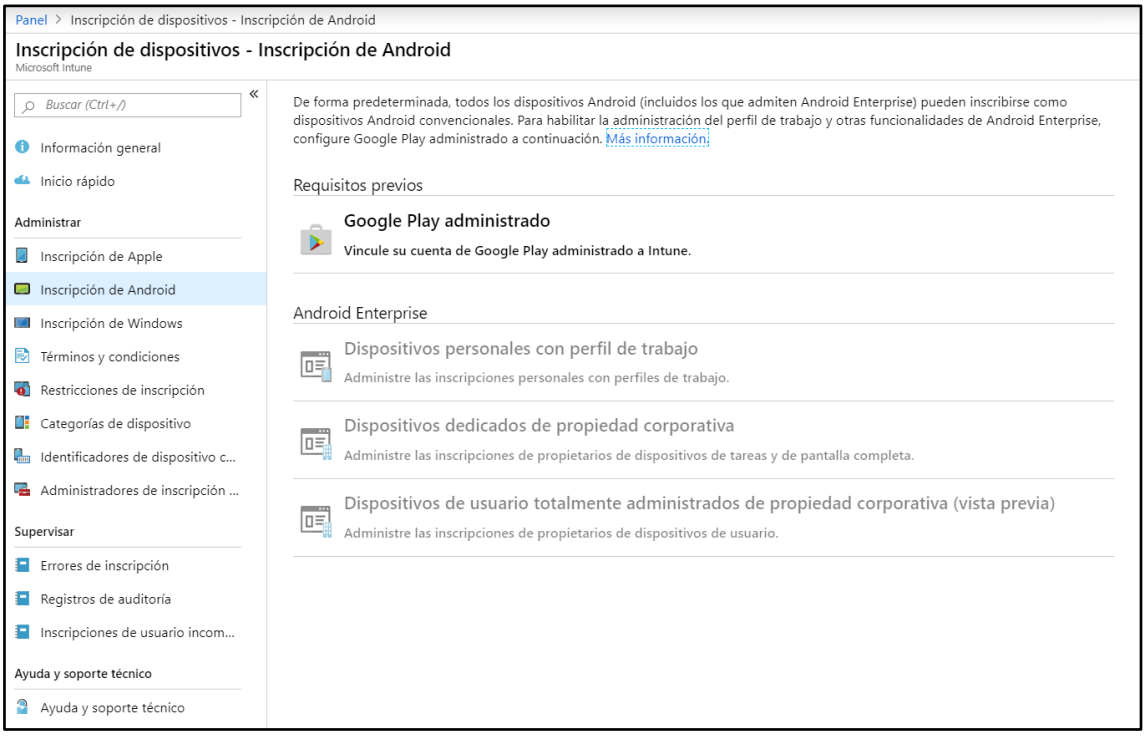
Panel de Administración de Grupos



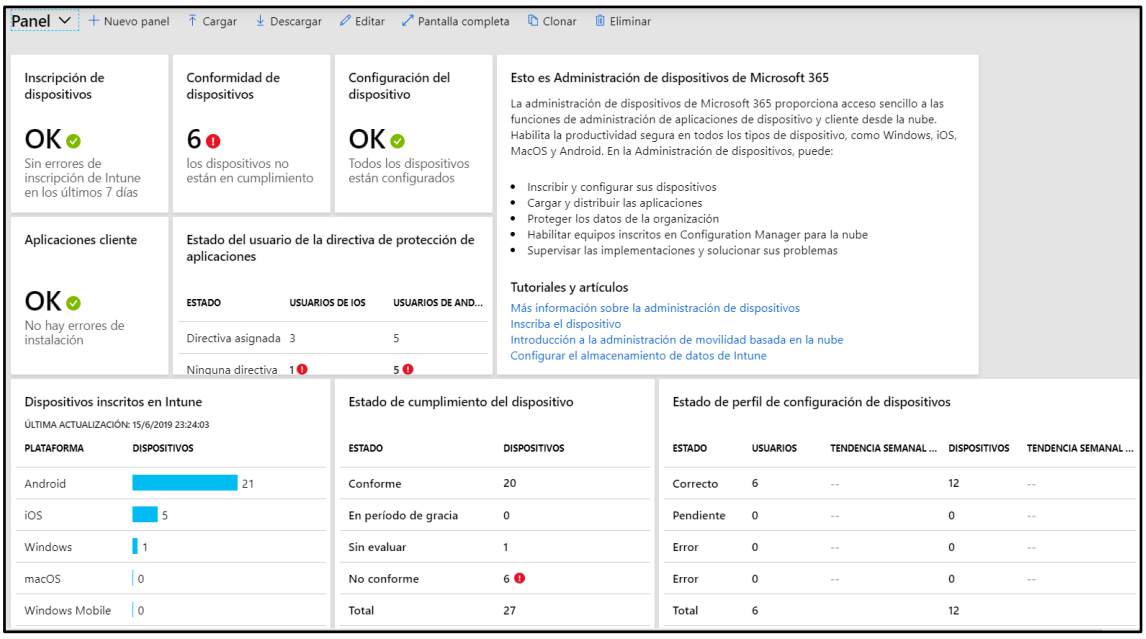
Portal de Intune - MDM



Plataforma de administración dispositivos



Plataforma de uso y control de dispositivos



Anexo 3: Artículo de investigación—carta de aceptación

UÍDE
Universidad Internacional del Ecuador
Extensión Guayaquil

CIIM 2019
IV CONFERENCIA INTERNACIONAL
DE INVESTIGACIÓN MULTIDISCIPLINARIA

Guayaquil, 27 de junio de 2019

Rupay Velazco Merlin Stefanny
Correa Rosales César Marcelo
Rivas Flores Kiara Alessandra
Salvatierra Garamendi Miriam Erica

Universidad Privada Norbert Weiner

Estimados autores,

Nos complace comunicarles que después de analizar el resumen de su ponencia: **Propuesta de políticas para reducir el riesgo de pérdida de información en la plataforma Cloud office 365 en una empresa comercial**, el Comité Científico de la IV CONFERENCIA INTERNACIONAL DE INVESTIGACIÓN MULTIDISCIPLINARIA considera que reúne las condiciones para ser aceptados como ponentes en el evento.
Para publicar su trabajo en Innova, deberán enviarlo hasta el 12 de julio para el proceso de revisión de la revista, para ser evaluado con el sistema de revisión de par ciego.

La conferencia se realizará, en el Hotel Sheraton de Guayaquil el 16 y 17 de julio de 2019. Para obtener información más detallada sobre la conferencia y alojamiento, por favor ingresar a la página web de la CIIM www.ciim-uide.com

Nos sentiremos honrados de compartir con ustedes estos días de intercambio de experiencias y sirva además este marco, para debatir reflexiones y criterios en torno a los ejes temáticos del evento.

Gracias por participar en la Conferencia Internacional de Investigación Multidisciplinaria 2019.

Comité Científico

CIIM 2019

Anexo 4: Instrumento cuantitativo

Universidad Norbert Wiener

Ficha de registro documental

Título del documento:	Recopilación de datos de movimientos sísmicos	
Período o año:	03/03/2019 al 03/05/19	
Objetivo del documento:	**Descripción del documento:**	**El documento responde al área de:**
Recopilación de datos de los acelerómetros en distintos movimientos telúricos	Este documento cuenta con la recopilación de datos de los periodos 03/03/2019 al 03/05/19 en que se originaron movimientos telúricos	La documentación hace mención del área del proyecto REDACIS, dedicado a la recopilación de datos de los diversos movimientos telúricos.

Registro de accesos mail box internos y externos.

Usuarios	Consulta	Client IP	Aplicativo	acceso externo
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user2@replica.com.pe	MailboxLogin	179.6.192.158	Microsoft.Exchange.Mapi	true

Anexo 5: Instrumento cualitativo

Ficha de entrevista

Datos básicos:

Cargo o puesto en que se desempeña	Jefe de ATP
Nombres y apellidos	Andrea Chang
Código de la entrevista	Entrevistado 3 (Entv.3)
Fecha	
Lugar de la entrevista	

Nro.	Preguntas de la entrevista
1	¿La información de la empresa está protegida con políticas de seguridad de la información?
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa?
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control?
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa?
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa?
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización?

Observaciones

.....
.....
.....

Ficha de entrevista

Datos básicos:

Cargo o puesto en que se desempeña	Gerente General
Nombres y apellidos	Felipe Garcés
Código de la entrevista	Entrevistado1 (Entv.1)
Fecha	
Lugar de la entrevista	

Nro.	Preguntas de la entrevista
1	¿La información de la empresa está protegida con políticas de seguridad de la información? Sustente su respuesta
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa? Sustente su respuesta
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control? Sustente su respuesta
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa? Sustente su respuesta
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa? Sustente su respuesta
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización? Sustente su respuesta

Observaciones

.....
.....
.....

Anexo 6: Base de datos

Universidad Norbert Wiener

Ficha de registro documental

Título del documento:	Recopilación de datos de movimientos sísmicos	
Período o año:	03/03/2019 al 03/05/19	
Objetivo del documento:	**Descripción del documento:**	**El documento responde al área de:**
Recopilación de datos de los acelerómetros en distintos movimientos telúricos	Este documento cuenta con la recopilación de datos de los periodos 03/03/2019 al 03/05/19 en que se originaron movimientos telúricos	La documentación hace mención del área del proyecto REDACIS, dedicado a la recopilación de datos de los diversos movimientos telúricos.

Registro de accesos mail box internos y externos.

Usuarios	Consulta	Client IP	Aplicativo	acceso externo
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false

user2@replica.com.pe	MailboxLogin	179.6.192.158	Microsoft.Exchange.Mapi	true
user2@replica.com.pe	MailboxLogin	179.6.192.158	Microsoft.Exchange.Autodiscover	true
jmalvarez@replica.com.pe	MailboxLogin	190.239.37.75	Microsoft.Exchange.WebServices	true
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user3@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user3@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
lramos@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user7@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user3@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
evertiz@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user8@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false

ventas4@replica.com.pe	MailboxLogin	181.224.246.25	\/owa\/SuiteServiceProxy.aspx	false
user2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ccalvo@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.OfflineAddressBook	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.OfflineAddressBook	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ccalvo@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
lramos@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ccalvo@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ccalvo@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
lramos@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	\/owa\/SuiteServiceProxy.aspx	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false

ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user5@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user5@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user5@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
ventas1@replica.com.pe	MailboxLogin	181.224.246.25	\/owa\/SuiteServiceProxy.aspx	false
user8@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user3@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
user7@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
marketing@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
lramos@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
marketing@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user7@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
user7@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false

rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
contabilidad@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user7@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
ventas4@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
ventas2@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
marketing@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
facturacion@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
bi@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
user8@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
jmalvarez@replica.com.pe	MailboxLogin	190.239.37.75	Microsoft.Exchange.WebServices	true
marketing@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Autodiscover	false
rbedrinana@REPLICA.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false
user1@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.WebServices	false

user3@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false
user6@replica.com.pe	MailboxLogin	181.224.246.25	Microsoft.Exchange.Mapi	false

Auditoria de Archivos de OneDrive y SharePoint

UserIds	Operaciones	Plataforma	IP	Aplicación
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.75	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.75	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user3@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 19.002.0107.0008 ship
user3@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 19.002.0107.0008 ship
user3@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 19.002.0107.0008 ship
user2@replica.com.pe	FileDownloaded	SharePoint	181.224.251.226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePoint	181.224.251.226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePoint	181.224.251.226	Mozilla\/5.0 (Windows NT 10.0
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93da5d20bec7b646388	FileDownloaded	OneDrive	200.37.228.225	Mozilla\/5.0 (Windows NT 10.0
cobranzas@replica.com.pe	FileDeleted	OneDrive	181.224.251.226	Microsoft SkyDriveSync

				18.240.1202.0004 ship
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93dda5d20bec7b646388	FileDownloaded	OneDrive	200.37.228.225	Mozilla\/5.0 (Windows NT 10.0
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93dda5d20bec7b646388	FileDownloaded	OneDrive	200.37.228.225	Mozilla\/5.0 (Windows NT 10.0
urn:spo:anon#ee48362d83475d5aeb86bb7bdd4ddb7e9d477f0936ec93dda5d20bec7b646388	FileDownloaded	OneDrive	200.37.228.225	Mozilla\/5.0 (Windows NT 10.0
user4@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user4@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user4@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user4@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user1@replica.com.pe	FileDeleted	OneDrive	190.236.8.235	OneDriveiOSApp\/10.52 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.75	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.75	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user2@replica.com.pe	FileDownloaded	SharePoint	181.224.251.226	Mozilla\/5.0 (Windows NT 10.0

user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user2@replica.com.pe	FileDownloaded	SharePo int	181.224.251 .226	Mozilla\/5.0 (Windows NT 10.0
user5@replica.com.pe	FileDeleted	SharePo int	181.224.251 .226	Microsoft SkyDriveSync 19.002.0107.0008 ship
user5@replica.com.pe	FileDeleted	SharePo int	181.224.251 .226	Microsoft SkyDriveSync 19.002.0107.0008 ship
ccalvo@replica.com.pe	FileDeleted	OneDriv e	181.224.251 .226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user1@replica.com.pe	FileDeleted	OneDriv e	181.224.251 .226	OneDriveiOSApp\/1 0.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDriv e	181.224.251 .226	OneDriveiOSApp\/1 0.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDriv e	190.232.110 .223	OneDriveiOSApp\/1 0.51.8 (iOS\/12.1.2
user3@replica.com.pe	FileDeleted	SharePo int	181.224.251 .226	Microsoft SkyDriveSync

				19.002.0107.0008 ship
user3@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 19.002.0107.0008 ship
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.54	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.54	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.54	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	OneDrive	190.232.110.54	OneDriveiOSApp\/10.51.8 (iOS\/12.1.2
user1@replica.com.pe	FileDeleted	SharePoint	181.224.251.226	Microsoft SkyDriveSync 18.240.1202.0004 ship
user5@replica.com.pe	FileDeleted	SharePoint	201.230.248.141	Microsoft SkyDriveSync 18.240.1202.0004 ship
user5@replica.com.pe	FileDeleted	SharePoint	201.230.248.141	Microsoft SkyDriveSync 18.240.1202.0004 ship
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"

urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"
urn:spo:anon#9f4b008963452dfc634667757e5b6f5a4096829bb05e61a315520fdae87cf10b	FileDownloaded	OneDrive	200.60.163.37	WebId:"0ba13fa9-86e7-4162-a44f-4182fddf3b32"

Fecha: ……Lugar: Portal nube

Anexo 7: Transcripción de las entrevistas o informe del análisis documental

Universidad Norbert Wiener

Ficha de entrevista

Datos básicos:

Cargo o puesto en que se desempeña	Gerente
Nombres y apellidos	Felipe G.
Código de la entrevista	Entrevistado1 (Entv.1)
Fecha	
Lugar de la entrevista	REPLICA

Nro.	Preguntas de la entrevista
1	¿La información de la empresa está protegida con políticas de seguridad de la información? Sustente su respuesta
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa? Sustente su respuesta
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control? Sustente su respuesta
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa? Sustente su respuesta
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa? Sustente su respuesta
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización? Sustente su respuesta

Observaciones

.....
.....
.....

Entrevistado1 (Entv.1)

Nro.	Preguntas de la entrevista	Respuestas
1	¿La información de la empresa está protegida con políticas de seguridad de la información? Sustente su respuesta	SI, se tienen políticas de seguridad establecidas como un Directorio Activo, Autenticación de Factores para los temas de correo y/o soluciones colaborativas y Seguridad para móviles.
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta	NO, se tienen implementadas, pero NO documentadas.
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa? Sustente su respuesta	SI, se tiene la política de poder impedir la salida de archivos, pero en nuestro caso muchos colaboradores tienen la opción de poder hacerlo dado que se necesita el trabajo colaborativo desde casa también.
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control? Sustente su respuesta	SI, porque la data sensible y por cumplir las normas como la Ley de Protección de Datos Personales debe mantener una política de control y seguridad de la información.
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa? Sustente su respuesta	Activar diferentes medios como la autenticación de factor para todas las cuentas, documentar y verificar cada área y usuario con el que se comparta la información y con quien se le de acceso a ver la información desde sus casas.
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa? Sustente su respuesta	Sí, dado que cada vez aumentan los ataques a servidores de correo tanto on premise como nube, y al colocar este sistema reduce las posibilidades de que personas con mala intención entren o bloqueen la información de la empresa.
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización? Sustente su respuesta	Activando políticas y sistemas tecnológicos como Data Loss Prevention, revisando las políticas usando Intunes y diferentes herramientas en el mercado diseñadas para este fin.

Entrevistado2 (Entv.2)

Nro.	Preguntas de la entrevista	Respuestas
1	¿La información de la empresa está protegida con políticas de seguridad de la información? Sustente su respuesta	Sí. Con políticas muy básicas como el respaldo de buzones de correo y de los datos confidenciales de la empresa.
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta	No, los colaboradores no están informados desde el principio de su contrato sobre los límites de la información a la que tendrán acceso y sobre la divulgación de ellos.
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa? Sustente su respuesta	No, no por escrita ni informada al colaborador.
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control? Sustente su respuesta	Por supuesto. Por dos motivos: los datos son confidenciales y porque la información pertenece a la empresa, mas no al individuo que colabora allí, por lo tanto, la divulgación debe ser sancionada.
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa? Sustente su respuesta	Sobre el acceso y uso de la información, divulgación y la propiedad intelectual.
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa? Sustente su respuesta	Sí, con la autenticación multifactor se obtendría dos aristas importantes: validar que el usuario es realmente la persona correcta y la empresa tendría conocimiento de la metadata del usuario que ingresó.
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización? Sustente su respuesta	Con la autenticación multifactor y obtener información desde dónde y con quién se está compartiendo la información

Entrevistado3 (Entv.3)

Nro.	Preguntas de la entrevista	Respuestas
1	¿La información de la empresa está protegida con políticas de seguridad de la información en Office 365? Sustente su respuesta	Si, actualmente se cuenta con medidas de seguridad, pero no completamente distribuidas entre las áreas involucradas.
2	¿Las políticas de la información se encuentran documentadas? Sustente su respuesta	No, actualmente no se cuenta con un documento donde se determinan las políticas de acceso y de restricción para el uso de la información de la empresa.
3	¿Cuentan con alguna política de información que impida la salida de archivos pertenecientes a la empresa? Sustente su respuesta	No, actualmente los usuarios puedes descargar su información desde cualquier lugar, ya que no cuenta con una restricción de acceso condicional.
4	¿Cree usted que cada documento que se comparta con data sensible que pertenece a la organización deba tener un control? Sustente su respuesta	Si, todos los archivos con data sensible deben tener un control exclusivo y con usuarios de confianza que los administren.
5	¿Qué políticas de información cree usted que puedan implementar para aumentar la seguridad en los archivos de la empresa? Sustente su respuesta	Restringir el acceso de los usuarios desde ubicaciones específicas, mejorar la autentificación de acceso a los usuarios de confianza, administración de la información en dispositivo que no pertenecen a la organización, configuración de archivos con plantillas de seguridad.
6	¿Usted cree que todos los usuarios deberían usar un sistema de autenticación multifactor para su cuenta corporativa? Sustente su respuesta	Si, lo usuarios que administración información sensible dentro de la organización deben contar con una capa más de seguridad para garantizar su identidad.
7	¿Cómo usted podría controlar la salida de archivos corporativos de la organización? Sustente su respuesta	Con la plataforma de office 365 podemos verificar los logs y crear políticas de seguridad dentro de la organización para controlar la descarga de información.

Anexo 8: Fichas de validación de los instrumentos cuantitativos

Universidad Norbert Wiener

Ficha de registro documental

Título del documento:	**Recopilación De Datos De Ataques A La Empresa Replica**
Período o año:	
Objetivo del documento:	**Descripción del documento:** / **El documento responde al área de:**
Recopilar datos de perdida de información en la empresa Replica	Este documento contara con la información de ataques y archivos perdidos. / Este documento pertenece al área de ATP, que cuenta con la información de perdida de datos.

No.	PERIODO	ASUNTO	PARES DE DOMINIOS			DIRECTIVA			REGISTRO DOCUMENTAL	ANALISIS
			ALTO	MEDIO	NORMAL	SUPLANTACION	ANTIMALWARE	ANTIPIAM		
1	Semana 1	Facturas	2			3	2	2	Portal O365	
	Semana 1	Ordenes de compra		3		2	1	4	Portal O365	
	Semana 2	Facturas	3	1	2	1	3	2	Portal O365	
2	Semana 2	Ordenes de compra	1	2		4	2	1	Portal O365	

Fecha: ..... Lugar: .....

Anexo 9: Evidencia de la visita a la empresa

Anexo 10: Matrices de trabajo

1. Matriz de causa efecto para definir el problema

CAUSA	SUBCAUSA	¿POR QUE?	EFECTO (CATEGORIA PROBLEMA)
C1. Personal	1. USO	1. Registrar su información personal en páginas fraudulentas.	SEGURIDAD DE LA INFORMACION
		2. Acceder a paginas fraudulentas.	
	2. INFORMACION	3. Brindar accesos sin restricciones a usuarios externos.	
		4. Abrir archivos en lugares no seguros.	
	3. LEALTAD	5. Incumplir con la ética personal sobre la información de la empresa	
		6. Vender la información a la competencia.	
C2. Equipos o dispositivo	4. CONTROL	7. Extraer información en dispositivos no permitidos	
		8. Hurto o perdida de dispositivo.	
	5. ACCESIBILIDAD	9. Acceder a la información de la empresa desde lugares públicos.	
		10. Vulnerar el acceso a los usuarios en sus dispositivos.	
	6. VULNERABILIDAD	11. No usar software de seguridad para la protección del equipo	
		12. Usar aplicativos de terceros o piratas.	
C3. Procesos o métodos	7. PROTECCION DE DATOS	13. Atacar a usuarios finales por personas malintencionadas	
		14. Ingresar de lugares no confiables	
	8. RESTRICCIONES	15. Falta de control sobre los dispositivos de uso diario.	
		16. Inicios de sesión no autorizados o permitidos.	
	9. ADMINISTRAR	17. Falta de seguridad en accesos y contraseñas de usuarios.	
		18. Equipos y descargas de información	
C3. Office 365	10. LICENCIAMIENTO	19. Adquirir licencias básicas.	
		20. Conocer los tipos de licencias adquiridas	
	11. SEGURIDAD	21. Configurar características de protección de datos	
		22. Activar auditorias y configurar alertas	
	12. DISPONIBILIDAD	23. Acceder desde cualquier dispositivo.	
		24. Establecer personal de confianza para administrar la plataforma	

2. Problema, objetivo, hipótesis

Problema general	Objetivo general	Hipótesis general
¿Cómo aumentar la protección de la información en la empresa Replica dentro de la plataforma de Office 365 de sus usuarios?	Proponer políticas de seguridad de la información que utilizan en la empresa Replica.	Las políticas de seguridad protegerán con un 70% la documentación de la empresa Replica SRL.
Problemas específicos	**Objetivos específicos**	
¿Cómo es la protección de la información en la empresa Replica?	Analizar las políticas de seguridad en la empresa Replica S.R.L.	
¿Cuáles son los factores/causas de mayor inseguridad en la empresa replica?	Explicar las causas de mayor demanda la seguridad de la información en la empresa Replica.	
¿Como las estrategias influyen en la seguridad de la información?	Predecir la influencia de las políticas de seguridad en la empresa Replica.	

3. Justificación

Justificación teórica		
Cuestiones	**Respuesta**	**Redacción final**
¿Qué teorías sustentan la investigación?	La teoría General de sistemas, La teoría de las políticas de información	La teoría General de sistemas nos ayudara en el trabajo de investigación en la implementación de las políticas de privacidad de los datos de la empresa
¿Cómo estas teorías aportan a su investigación?	La teoría general de sistemas ayudara a determinar cuáles son los procesos que podremos segmentar de tal manera el inicio del problema. La teoría de las políticas de información nos ayudara a reducir las pérdidas de información.	La teoría general de sistemas ayudara a determinar cuáles son los procesos que podremos segmentar de tal manera el inicio del problema. La teoría de las políticas de información nos ayudara a reducir las pérdidas de información.
Justificación práctica		
¿Por qué hacer el trabajo de investigación?	El trabajo de investigación nos ayudara a mejorar la seguridad de los datos corporativos, implementaremos políticas de seguridad que permitan aumentar la confiabilidad de la información.	De acuerdo con los objetivos de la investigación implementaremos políticas de seguridad que permitan aumentar la confiabilidad de la información, para ello los procedimientos en el uso de la plataforma se verán afectados con el objetivo de preservar un uso adecuado y seguro en los datos a los que el usuario tiene acceso. Por otro lado, se busca que este acceso a la información de la organización sea con métodos adicionales de autenticidad.

¿Cuál será la utilidad?	La utilidad es mejorar la seguridad de la información corporativa.	La utilidad es mejorar la seguridad de la información corporativa que se comparte desde la plataforma Cloud, agregando políticas de seguridad.
¿Qué espera con la investigación?	Aumentar el control de la información corporativa utilizada por Office 365.	Aumentar el control de la información corporativa utilizada por la plataforma cloud, que nos permite almacenar archivos y compartirlos.
Justificación metodológica		
¿Por qué investiga bajo ese diseño?	Según el estudio que se va a realizar por medio del análisis realizado se determinó que se utilizará una investigación holística con un enfoque mixto, presentando un estudio global para obtener resultados más acertados que nos permitirá asegurar la información involucrada en los procesos, obteniendo sus causas y efectos sobre la información que utilizan los empleados, y esto nos permitirá obtener una solución propicia para este estudio.	Se determina utilizar el estudio de investigación holística que usará un enfoque mixto, presentando un estudio para obtener resultados acertados que nos permitirá asegurar los procesos correctos, de tal manera determinar las causas y efectos sobre la información corporativa que utilizan los empleados, y esto nos permitirá obtener una solución propicia para mejorar la seguridad de los archivos corporativos.
¿El resultado de la investigación permitirá resolver algún problema?	La investigación que se realizara nos ayudara aumentar la seguridad de los datos corporativos, y tener un mejor control sobre los datos que se comparten.	La investigación que se realizara nos ayudara aumentar la seguridad de los datos corporativos, y tener un mejor control sobre los datos que se comparten.

4. Matriz de teorías

Teoría 1: Teoría general de Sistemas				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ángel A. Sarabia	1995	Según Sarabia (1995) indican que: La Teoría General de Sistemas (T.G.S.) es la historia de una filosofía y un método para analizar y estudiar la realidad y desarrollar modelos, a partir de los cuales puedo intentar una aproximación paulatina a la percepción de una parte de esa globalidad que es el Universo, configurando un modelo de la misma no aislado del resto al que llamaremos sistema.	La Teoría General de Sistemas (T.G.S.) es la historia de una filosofía y un método que ayuda al análisis y estudio de la realidad y desarrollo de modelos, a partir de los cuales se puede intentar una aproximación paulatina a la percepción de una parte de esa globalidad que es el Universo, se configura un modelo de la misma no aislado del resto al que llamaremos sistema.. (Sarabia, 1995)	
Referencia:	**http://roa.ult.edu.cu/bitstream/123456789/3297/2/La%20Teor%3Fa%20General%20de%20Sistemas%20-%20%3Fngel%20A.%20Sarabia-FREELIBROS.ORG.pdf**			
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Alonso Tamayo Álzate	1999	se trata de una concepción estructurada o metodología que tiene como propósito estudiar el sistema como un todo, de forma íntegra, tomando como base sus componentes y analizando las relaciones e interrelaciones existentes entre éstas y mediante la aplicación de estrategias científicas, conducir al entendimiento	Se trata de estructura o metodología que tiene como propósito estudiar el sistema como un todo, de forma íntegra, que toma como base sus componentes y analiza las relaciones e interrelaciones existentes y mediante la aplicación de estrategias científicas, conduce al entendimiento globalizante y generalizado del sistema. (Tamayo, 1998)	

		globalizante y generalizado del sistema. (p.86)		
Referencia:	**http://bdigital.unal.edu.co/57900/1/teoriageneraldesistemas.pdf**			
Autor/es	**Año**	**Cita**	**Parafraseo**	
Alonso Tamayo Álzate	1999	"La Teoría General de sistemas se concibe como una serie de definiciones, de suposiciones y de proposiciones relacionadas entre sí por medio de las cuales se aprecian todos los fenómenos y los objetos reales como una jerarquía integral de grupos formados por materia y energía; estos grupos son los sistemas."	"La Teoría General de sistemas se inicia como un conjunto de definiciones, de suposiciones y de proposiciones que se relacionan por medio de las cuales se aprecia todos los fenómenos y los objetos reales como una escala integral de grupos formados por materia y energía; estos grupos son los sistemas."	
Referencia:	**http://bdigital.unal.edu.co/57900/1/teoriageneraldesistemas.pdf**			

Teoría 2: Teoría General de la Información				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ángel Benito	**1997**	La Teoría General de la Información es la disciplina más amplia de cuantas se ocupan del hecho social de la información y comunicación	La Teoría General de la Información es una disciplina amplia de cuantas se ocupan del hecho social de la información y comunicaciones colectivas. Una ciencia	

		colectivas. Es una ciencia nueva, básica, imprescindible para una comprensión acabada del fenómeno contemporáneo que hemos convenido en llamar comunicaciones de masas (p.14)	nueva, básica, imprescindible para comprender luego del fenómeno contemporáneo que ha convenido en llamar comunicaciones de masas. (Benito Jaén, 1981)	
Referencia:	**https://www.infoamerica.org/teoria_articulos/benito01.pdf**			
Autor/es	**Año**	**Cita**	**Parafraseo**	
Alejandro López, Andrea Parada, Franco Simonetti	**1995**	Según López, Parada & Simonetti (1995) indican que: A partir de la acelerada difusión y especialización que experimentan los medios de comunicación en el procesamiento y transmisión de información durante la primera mitad de nuestro siglo, se desarrolla el primer modelo científico del proceso de comunicación conocido como la Teoría de la Información o Teoría Matemática de la Comunicación. Específicamente, se desarrolla en el área de la telegrafía donde surge la necesidad de determinar, con la	A partir del cambio de difusión y especialización que muestran los medios de comunicación en el procesamiento y cambio de información durante la primera mitad de nuestro siglo, se construye el primer modelo científico del proceso de comunicación conocido como la Teoría de la Información o Teoría Matemática de la Comunicación. Específicamente, se desarrolla en el área de la telegrafía donde nace la necesidad de determinar, con una gran precisión, la capacidad de los diferentes sistemas de comunicación para transmitir información. (Lopez, Parada, & Simonetti, 1995)	

		máxima precisión, la capacidad de los diferentes sistemas de comunicación para transmitir información.		
Referencia:				

5. Matriz de antecedentes

Datos del antecedente internacional: 1		**Redacción final**
Título	*Análisis en seguridad informática y seguridad de la información basado en la norma iso/iec 27001 - sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros*	Según el estudio de Bermúdez y Bailón (2015) referente a la *Análisis en seguridad informática y seguridad de la información basado en la norma iso/iec 27001 - sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros, identifico su objetivo principal a*nalizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas a garantizar la confidencialidad, integridad y disponibilidad de la información mediante la formulación recomendaciones de seguridad y controles basados en la norma ISO/IEC27001, La metodología a continuación propuesta está alineada a la norma ISO/IEC 27001 y corresponde al análisis de seguridad de la información y seguridad informática realizado, el cual empezó con la identificación de las vulnerabilidades de la situación actual, así como la evaluación de amenazas, vulnerabilidades, impacto y riesgo de los activos de información de las áreas que son consideradas críticas de Credigestión, En conclusión, el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja potenciales índices de riesgos, los cuales exponen a la información a daños, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio.
Autor	Bermúdez y Bailón	
Año	**2015**	
Objetivo	**Analizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas a garantizar la confidencialidad, integridad y disponibilidad de la información mediante la formulación recomendaciones de seguridad y controles basados en la norma ISO/IEC27001**	

Metodología		La metodología a continuación propuesta está alineada a la norma ISO/IEC 27001 y corresponde al análisis de seguridad de la información y seguridad informática realizado, el cual empezó con la identificación de las vulnerabilidades de la situación actual, así como la evaluación de amenazas, vulnerabilidades, impacto y riesgo de los activos de información de las áreas que son consideradas críticas de Credigestión,
	Tipo	**Tipo de investigación de campo** **Tipo de investigación descriptiva** **Tipo de investigación no experimental,** **Tipo de investigación explicativa**
	Enfoque	
	Diseño	
	Método	
	Población	**Universo**
	Muestra	**Directivo del departamento, Operario**
	Técnicas	
	Instrumentos	
	Método de análisis de datos	
Resultados		

Conclusiones	
Referencia (tesis)	https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Datos del antecedente internacional: 1		
Título		*Gestión De La Ciberseguridad Y Prevención De Los Ataques Cibernéticos En Las Pymes Del Perú, 2016*
Autor		Vasquez Pajuelo
Año		**2016**
Objetivo		*Determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016.*
Metodología		**Holística**
	Tipo	**básica**
	Enfoque	**cuantitativo**
	Diseño	No Experimental
	Método	
	Población	1.713.272 empresas
	Muestra	Transporte Zavala Cargo S.A.C.
	Técnicas	para la recolección de datos utilizaremos la Técnica Indirecta.

Redacción final

Según Vasquez Pajuelo (2016) en el estudio de *Gestión De La Ciberseguridad Y Prevención De Los Ataques Cibernéticos En Las Pymes Del Perú, 2016,* cuyo objetivo fue determinar la gestión de la ciberseguridad con la prevención de los ataques cibernéticos en las PYMES del Perú, 2016. Mediante la encuesta utilizada se obtuvo los resultados generales que se derivan de la encuesta demuestran que para el personal consultado de la Empresa Transporte Zavala Cargo S.A.C., la ciberseguridad es importante; sin embargo la empresa no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus empleados en materia de ciberseguridad para prevenir y evitar posibles amenazas; no invierten en herramientas de ciberseguridad y no tienen personal responsable de la seguridad de la empresa en la red.

	Instrumentos	utilizaremos La Encuesta como instrumento de recolección de datos.
	Método de análisis de datos	
Resultados		
Conclusiones		
Referencia (tesis)		**http://repositorio.usil.edu.pe/bitstream/USIL/2810/1/2017_Inoguchi_Gestion-de-la-ciberseguridad.pdf**

Datos del antecedente internacional: 1		
Título		Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo
Autor		Julio Cesar Alcántara Flores
Año		**2015**
Objetivo		Contribuir a mejorar el nivel de seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo.
Metodología		**Holística**
	Tipo	**No probabilístico**
	Enfoque	**cuantitativo**
	Diseño	

Redacción final

Según Alcántara (2015) en el estudio de la *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo,* su objetivo general Contribuir a mejorar el nivel de seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo, mediante el estudio y encuestas realizadas se obtuvieron los resultados de la Tesis, daremos a conocer los distintos entregables asociados a la norma ISO/IEC 27001, que se consideraron para el desarrollo realizado en la Institución policial PNP "Comisaria del Norte" – de la ciudad de Chiclayo. A continuación, mencionaremos una lista de los distintos entregables, que posteriormente se detallarán respectivamente en el documento.

	Método	
	Población	30 trabajadores
	Muestra	**No probabilístico**
	Técnicas	
	Instrumentos	**Ficha de observación, reportes**
	Método de análisis de datos	
Resultados		
Conclusiones		
Referencia (tesis)		**http://tesis.usat.edu.pe/bitstream/usat/539/1/TL_Alcantara_Flores_JulioCesar.pdf**

Datos del antecedente internacional: 1		**Redacción final**
Título	Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño	Yáñez (2017) *Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño,* El objetivo general de la Tesis, es definir e implementar un conjunto de sistemas basados en software open source para crear un SGSI de costo asequible, que cumpla con la normativa indicada en la ISO27001:2013, bajo una estrategia de mejora continua de procesos en una institución pública. Holística, La elaboración de este proyecto de implementación de un SGSI que detalla la presente tesis, logró un cambio del enfoque de lo que la unidad de sistemas entendía como seguridad de la información, desde una mirada solo de seguridad informática a un concepto más amplio y de carácter estratégico para la organización: la necesidad de proteger la información como el activo valioso. Este nuevo enfoque permitió la implementación de nuevas políticas y procesos de control, que sientan las bases para la creación de sistemas que monitorean y aseguran la mejora continua de las políticas y procedimientos definidos.
Autor	Nelson Alejandro Yáñez Cáceres	
Año	**2017**	
Objetivo	El objetivo general de la Tesis es definir e implementar un conjunto de sistemas basados en software open source para crear un SGSI de costo asequible, que cumpla con la normativa indicada en la ISO27001:2013, bajo una estrategia de mejora continua	

		de procesos en una institución pública.
Metodología		**Holística**
	Tipo	**No probabilístico**
	Enfoque	**cuantitativo**
	Diseño	
	Método	
	Población	
	Muestra	
	Técnicas	
	Instrumentos	
	Método de análisis de datos	
Resultados		
Conclusiones		La elaboración de este proyecto de implementación de un SGSI que detalla la presente tesis logró un cambio del enfoque de lo que la unidad de sistemas entendía como seguridad de la información, desde una mirada solo de seguridad informática a un concepto más amplio y de carácter estratégico para la organización: la necesidad de proteger la información como el activo valioso. Este nuevo

	enfoque permitió la implementación de nuevas políticas y procesos de control, que sientan las bases para la creación de sistemas que monitorean y aseguran la mejora continua de las políticas y procedimientos definidos.	
Referencia (tesis)	**http://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y**	

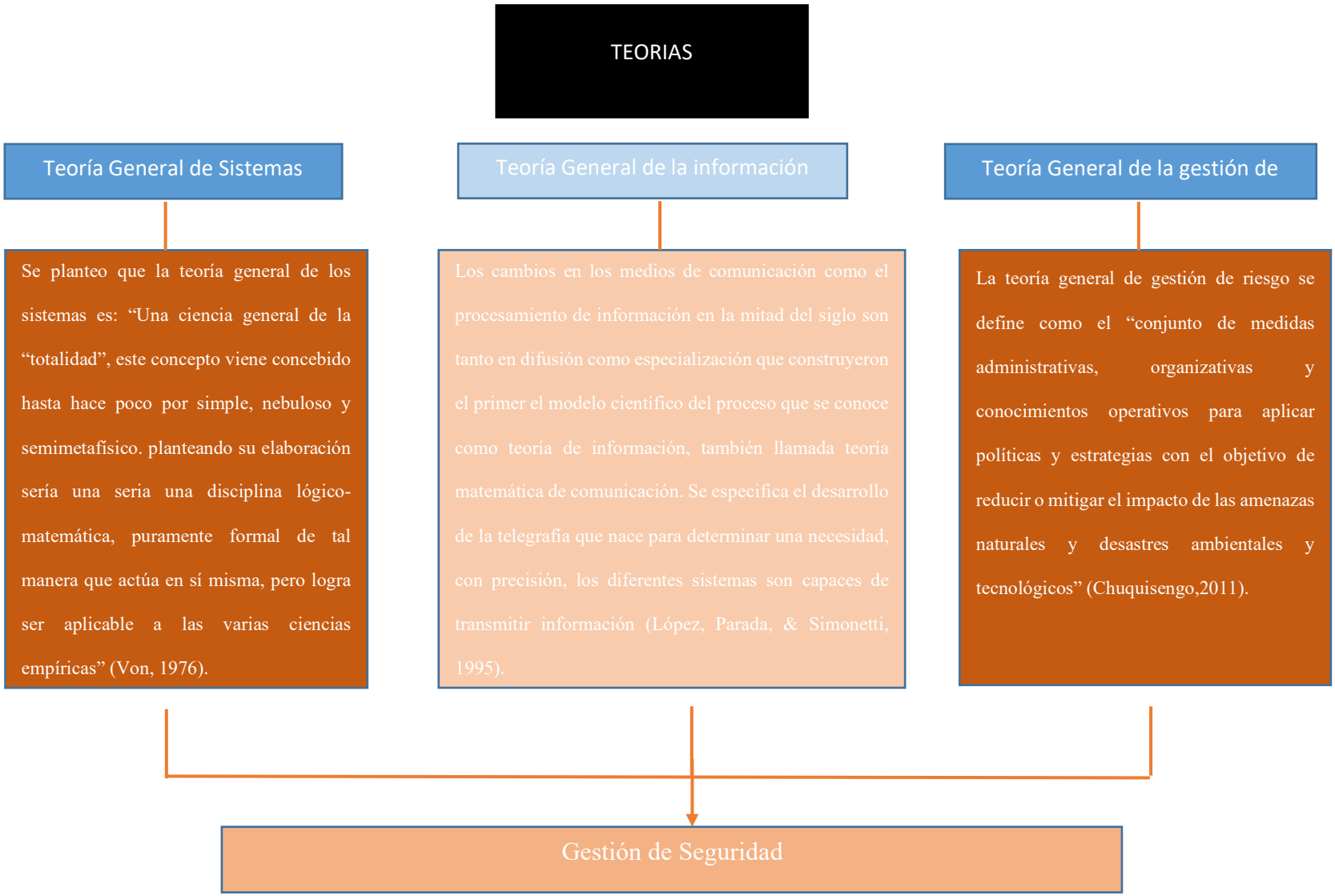
6. Marco conceptual

Variable o categoría 1: Gestión de Seguridad				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Rubén Alejandro Rayme Serrano	**2007**	Según Rayme (2017) , La gestión de la seguridad de la información consiste en garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.	La seguridad de la información trata de garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por las entidades de negocio de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Rayme Serrano, 2007)	
Referencia:	**http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/428/Rayme_sr.pdf?sequence=1**			
Autor/es	**Año**	**Cita**	**Parafraseo**	
Carlos Ojeda	**2015**	Consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua; incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora, con el objetivo de anticipar, reconocer, evaluar y controlar los	Se trata del desarrollo de un procedimiento lógico y por periodos, se basan en la mejora continua; que engloba la política, la aplicación, la evaluación, y los cambios de mejora, con el propósito de anticipar, examinar, evaluar y comprobar los riesgos que puedan perjudicar la	

		riesgos que puedan afectar la seguridad y la salud en el trabajo.	seguridad y la salud en su ocupación. (Ojeda, 2017)	
Referencia:	**http://www.infotephvg.edu.co/cienaga/hermesoft/portalIG/home_1/recursos/julio_2017/05072017/manual-sst.pdf**			
Variable o categoría 1: Riesgo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jorge Albarracín	**2002**	Según Albarracín (2002), La sociedad del riesgo es una nueva forma social que surge como consecuencia de la modernización de la sociedad industrial. De acuerdo con este paradigma, el nacimiento de esta nueva forma social no se produce por un estallido político, sino como consecuencia de la propia modernización de la sociedad industrial	La sociedad del riesgo es nueva manera social que brota como resultado de la actualización de la sociedad industrial. De acuerdo con esta pauta, el origen de esta apariencia social no se elabora por un estallido político, de tal manera la consecuencia de la modernización. (Albarracín, 2002)	
Referencia:	**http://biblioteca.clacso.edu.ar/Bolivia/cides-umsa/20120903104211/albarra.pdf**			
Autor/es	**Año**	**Cita**	**Parafraseo**	
Luz Mery Guevara	**2012**	Según Guevara (2012), Un proceso de gestión de riesgo va a permitir a la organización entender cuál es su situación de seguridad actual, le va a facilitar tomar decisiones adecuadas para mitigar los riesgos; también evaluar qué medidas se implementan a largo y corto plazo y al final precisará si las decisiones fueron las correctas.	Un proceso de gestión de riesgo debe permitir que la organización entienda cuál es su situación actual de seguridad, le facilitara tomar decisiones para mitigar los riesgos; de la misma forma evaluar que las medidas que se implementen a largo y corto plazo, al final especificar si las decisiones fueron las correctas. (Parra Moreno, 2012)	
Referencia:	**https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf;jsessionid=17F4BBCA76C61725122D03185D6CE6F4?sequence=2**			
Variable o categoría 1: Control				
Autor/es	**Año**	**Cita**	**Parafraseo**	
UCM		La teoría del control es una rama interdisciplinaria de la ingeniería y de las matemáticas, que trata con sistemas dinámicos y que depende y comparte herramientas con la física (dinámica y modelado de sistemas), los computadores (información y software), la investigación operativa (optimización y teoría de juegos) y la	El control es una rama interdisciplinaria de la ingeniería y de las matemáticas, se trata como practicas dinámicas, estas dependen y comparten herramientas con la física, los equipos de escritorio, la investigación operativa y la IA, de las cuales se vacían instrumentos y metodologías que	

		inteligencia artificial, de las cuales se extraen herramientas y metodologías que permiten ir ampliando las posibilidades del control.	nos permita ampliar la posibilidad del control. (UCM, 2019)	
Referencia:	**https://informatica.ucm.es/data/cont/docs/titulaciones/184.pdf**			
Autor/es	**Año**	**Cita**	**Parafraseo**	
Félix Armando Fermín Pérez	**2011**	Según Armand & Pérez (2011). El control es un enfoque sistemático de análisis y diseño de controladores, que se fundamenta en el uso de las matemáticas. Utiliza conceptos tales como el de función de transferencia, que relaciona la salida y entrada de un sistema en particular para estudiar sus propiedades.	El control es como un enfoque metódico de análisis y planeamiento de controladores, que se fundamentan en el uso de la matemática. Se usan conceptos para la función de claridad, que vincula la salida y entrada de un método característico para evaluar sus propiedades**.** (Fermín, 2012)	
Referencia:				

7. Construcción de la categoría problema



8. Matriz del método

Enfoque				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández Sampieri, Carlos Fernández Collado, María del Pilar Baptista Lucio.	**2010**	enfoque mixto se exploran distintos niveles del problema de estudio. Incluso, podemos evaluar más extensamente las dificultades en nuestras indagaciones, ubicados en todo el proceso de investigación y en cada una de sus etapas	Este enfoque nos permite evaluar el nivel del problema de la investigación. Podemos determinar cuáles son nuestros puntos de dificultad, como en nuestros procesos que utilizamos para la investigación y en cada etapa de nuestro desarrollo.	Nos ayudara a responder nuestro planteamiento del problema, utilizando la data recolectada de método cualitativo y cuantitativo, con estos datos podremos determinar los mejores procesos para brindar una solución para nuestra empresa.
Referencia:	**http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf**			
Tipo proyectiva				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jacqueline Hurtado de Barrera	**2000**	Proyectiva, todas aquellas investigaciones que conducen a inventos, programas, diseños o a creaciones dirigidas a determinada necesidad, y basadas en conocimientos anteriores.	El todo de investigación proyectiva se basa en la búsqueda de plantear diversas soluciones a un determinado problema basándose en conocimientos anteriores sobre la problemática propuesta.	Gracias a que se usará el método proyectivo permitirá a este trabajo poder plantear diversas alternativas de solución teniendo como sustento investigaciones anteriores como sustento razonable.
Referencia:	https://drive.google.com/file/d/1pC0PzBO3mB-qUH8Z31cm8nDe4l_wraK-/view			
Nivel comprensivo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jacqueline Hurtado de Barrera	**2000**	En el nivel comprensivo se estudia al evento en su relación con otros eventos, dentro de un tema mayor, enfatizado por lo general las relaciones de causalidad, aunque no exclusivamente; los objetivos propios de este nivel son explicar y proponer	El nivel comprensivo nos permite estudiar la relación con otros eventos como un todo que enfatiza por lo general en relaciones de causalidad, aunque no exclusivamente donde se llega a los niveles de explicar y proponer.	El nivel compresivo nos permitirá ver las relaciones existentes entre las diversas partes del todo teniendo como resultado un estudio con la capacidad de proponer y explicar los objetivos trazado en la investigación.
Referencia:	https://drive.google.com/file/d/1pC0PzBO3mB-qUH8Z31cm8nDe4l_wraK-/view			
Método inductivo y deductivo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández	**2010**	Dentro del enfoque deductivo-cuantitativo, las hipótesis se contrastan	En el enfoque deductivo tiene como cualidad que la hipótesis tiene que ser	Parea poder validad la hipótesis propuesta no solo se deberá establecer

Sampieri, Carlos Fernández Collado, María del Pilar Baptista Lucio.		con la realidad para aceptarse o rechazarse en un contexto determinado. Asimismo, se explica el papel que juegan la literatura y las hipótesis en el proceso inductivo; del mismo modo, cómo se inicia, en la práctica, un estudio cualitativo, mediante el ingreso al contexto, ambiente o campo.	validada para poder decir que es admitida o no, mientas que en el enfoque inductivo se evalúa el contexto del acontecimiento para validar la hipótesis propuesta.	los datos que reafirmen dicha hipótesis sino también se tendrá en cuenta el contexto y las circunstancias en la que se establece la propuesta.
Referencia:	**http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf**			

9. Población, muestra y unidades informantes

Población				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández Sampieri, Carlos Fernández Collado, María del Pilar Baptista Lucio.	**2010**	Es el conjunto de todos los casos que concuerdan con una serie de especificaciones.	La particularidad de los casos que suscitan bajo un conjunto de ellos es la población, que se determina de acuerdo con especificaciones.	Para nuestra investigación seleccionaremos una población con un tema relacionado entre sí, esto nos ayudara enfocándonos en el objetivo.
Número de xxxx:		##		
Referencia:	http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf			

Muestra				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández Sampieri, Carlos Fernández Collado, María del Pilar Baptista Lucio.	2010	Subgrupo de la población del cual se recolectan los datos y debe ser representativo de ésta.	Una parte de la población es la muestra de esta se seleccionan para recolectar los datos y estos deben representar en el estudio que se realiza.	Seleccionaremos la recolección de datos en este caso la recolección de datos es amplia por auditoria, usaremos una muestra de 2 meses de data seleccionada para evaluar nuestro objetivo.

Técnica de muestreo:	**Pegar la aplicación de la fórmula**		
Número de xxxx:	**##**		
Referencia:	**http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf**		

Unidades informantes				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández Sampieri, Carlos Fernández Collado, María del Pilar Baptista Lucio.	2010	Identificar informantes que aporten datos y nos guíen por el lugar, adentrarse y compenetrarse con la situación de investigación, además de verificar la factibilidad del estudio.	En el estudio se deben segmentar o identificar bien las unidades informantes ya que estas nos guiaran con la investigación de tal modo que se verifique la factibilidad de la investigación.	Se debe tener en cuenta cuales son los usuarios a los que entrevistaremos, ya que por medio de esta información recolectada verificaremos si tenemos fallas en nuestras políticas de seguridad y revisar si el área requiere mejorar la seguridad de la información.
Número de xxxx:		**##**		
Referencia:	**http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf**			

10. Técnicas e instrumentos

Técnica/s				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Jacqueline Hurtado de Barrera	2000	Las técnicas de recolección de datos comprenden procedimientos y actividades que le permiten al investigador obtener la información necesaria para dar respuesta a su pregunta de investigación.	La recopilación de datos tiene como técnica diversas actividades cuyo fin es de elaborar respuestas del investigador a través de la información recopilada.	Se hará uso de las técnicas de recopilación de información para poder obtener datos que nos ayuden a tener respuestas solidas a nuestros diversos cuestionamientos de la investigación.

Referencia:	https://drive.google.com/file/d/1pC0PzBO3mB-qUH8Z31cm8nDe4l_wraK-/view

Instrumento/s				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Roberto Hernández Sampieri	2010	Un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente los conceptos o las variables que el investigador tiene en mente.	Un adecuado instrumento de medición nos permite recopilar datos tangibles y nos permite reafirma las hipótesis que se propone en la investigación.	Este instrumento nos ayuda en cómo proceder con el grupo definido de estudio con las interrogantes determinadas de la investigación que deseamos conocer algo" (Sierra, 1994), puede tratarse de un plan, una forma de entrevista o una herramienta de cálculo. Aunque el cuestionario puede ser un procedimiento escrito para lograr datos, es posible adaptarlo verbalmente. (Corral, 2010).
Referencia:	http://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf			

Validez				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Gerardo Prieto y Ana Delgado	2010	La validez es un proceso de acumulación de pruebas para apoyar la interpretación y el uso de las puntuaciones. Por tanto, el objeto de la validación no es la prueba, sino la interpretación de sus puntuaciones en relación con un objetivo o uso concreto. El proceso de validación se concibe como un argumento que parte de una definición explícita de las interpretaciones que se proponen,	El proceso de la acumulación de pruebas que nos ayuden a interpretar la relación frente a un objetivo, que se puede interpretar de forma explícita de fundamentos teóricos y predicciones que se justifican científicamente.	Utilizamos la validez para medir la confiabilidad de nuestra investigación, revisando la información encontrada y los resultados de los análisis de datos realizados.

		de su fundamentación teórica, de las predicciones derivadas y de los datos que justificarían científicamente su pertinencia.		
	Apellidos y nombres		**Especialidad**	**Criterio de evaluación**
Validador 1				
Validador 2				
Validador 3				
Referencia:	http://www.redalyc.org/pdf/778/77812441007.pdf			

Confiabilidad				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Carlos Ruiz Bolívar	**2015**	Una de las características técnicas que determinan la utilidad de los resultados de un instrumento de medición es su grado de reproducibilidad. Esta se refiere al hecho de que los resultados obtenidos con el instrumento en una determinada ocasión, bajo ciertas condiciones, deberían similares si volviéramos a medir el mismo rasgo en condiciones idénticas.	Los datos deben haber sido obtenidos por un instrumento de forma determinada por condiciones generales o bajo condiciones que se determinaron en un inicio una forma de probarlo sería medir bajo un mismo rango de condiciones.	La confiabilidad se aplicará en nuestra investigación determinando las condiciones bajo las cuales podamos obtener los resultados que podamos volver a medir bajo los mismos parámetros que el inicial.
Prueba de confiabilidad			Criterio de evaluación:	Aplicable No aplicable
Valor calculado				
Referencia:	http://200.11.208.195/blogRedDocente/alexisduran/wp-content/uploads/2015/11/CONFIABILIDAD.pdf			

11. Procedimiento

Paso 1	**Recopilación de datos cuantitativos**
Paso 2	**Análisis de datos cuantitativos**
Paso 3	**Recopilación de datos cualitativos a través de entrevistas**
Paso 4	**Transcripción de las entrevistas**
Paso 5	**Análisis de las entrevistas en atlas ti**
Paso 6	**Triangulación de los resultados de las entrevistas con los resultados cuantitativos**

12. Análisis de datos

Cuantitativo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ruiz Manuel, Borboa Maria, Rodríguez Julio	**2013**	Uno de los pasos más importantes y decisivos de la investigación es la elección del método o camino que llevará a obtener de la investigación resultados válidos que respondan a los objetivos inicialmente planteados. De esta decisión dependerá la forma de trabajo, la adquisición de la información, los análisis que se practiquen y por consiguiente el tipo de resultados que se obtengan; la selección del proceso de investigación guía todo el proceso investigativo y con base en él se logra el objetivo de toda investigación.	Es uno de los análisis más importantes que pueden llegar a darnos la información para responder en los objetivos que se plantearon para la investigación, podemos aplicarla de maneras distintas como descriptivo o inferencial, generalmente se obtiene como una estructuración numérica de una o distintas variables y de esto se verán los tipos de análisis a practicar.	Usaremos el tipo de análisis cuantitativo para nuestro estudio, uno de estos tipos es la recolección de datos que aplicamos, para evaluar cómo se encuentran los accesos en nuestro portal, y como manejan la información los usuarios de la empresa.
Número de xxxx:		**##**		
Referencia:	http://www.eumed.net/rev/tlatemoani/13/estudios-fiscales.pdf			

Cualitativo				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ruiz Manuel, Borboa Maria, Rodríguez Julio	2013	Los autores Blasco y Pérez (2007:25), señalan que la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas. Utiliza variedad de instrumentos para recoger información como las entrevistas, imágenes, observaciones, historias de vida, en los que se describen las rutinas y las situaciones problemáticas, así como los significados en la vida de los participantes.	Al aplicar en nuestra investigación el análisis cualitativo, es utilizar a los implicados en el estudio para comprobar lo que sucede en su entorno, podemos obtener resultados de entrevistas, como describen su rutina de vida y de otros tipos de análisis.	Al aplicar el análisis cualitativo en nuestra investigación nos daremos cuenta si los administradores de la plataforma de la empresa Replica requieren de la solución que se plantea, para mejorar la seguridad de la información.
Número de xxxx:		**##**		
Referencia:	http://www.eumed.net/rev/tlatemoani/13/estudios-fiscales.pdf			

Mixto				
Autor/es	**Año**	**Cita**	**Parafraseo**	**Aplicación en su tesis**
Ruiz Manuel, Borboa Maria, Rodríguez Julio	**2013**	Al utilizar el enfoque mixto, se entremezclan los enfoques cualitativo y cuantitativo en la mayoría de sus etapas, por lo que es conveniente combinarlos para obtener información que permita triangularla. Esta triangulación aparece como alternativa a fin de tener la posibilidad de encontrar diferentes caminos para conducirlo a una comprensión e	El proceso del enfoque mixto nos ayuda con la recolección, análisis y vinculación de los datos cuantitativos y cualitativos en un mismo estudio lo cual nos permite responder a un planteamiento a través de una serie de investigaciones.	Se puede determinar que el enfoque mixto sería el apropiado, debido a que el enfoque cuantitativo nos facilitó incursionando en forma práctica en el juego de los números, tratamos la información empíricamente desde su origen, en la que se preparamos como primera instánciala recolección de datos que en nuestro caso es un log de auditoria, las cuales tienen

		interpretación lo más amplia del fenómeno en estudio.		variables dependientes e independientes de la investigación las cuales ligamos de una manera intima a los objetivos, con ello, se pretendemos usar estos resultados para conocer la percepción de los usuarios de la empresa Replica y poder corroborarlos con el Atlas TI.
Número de xxxx:		**##**		
Referencia:	http://www.eumed.net/rev/tlatemoani/13/estudios-fiscales.pdf			