ESCUELA DE POSTGRADO

Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú

Tesis para optar el grado **Maestro** en:

Ingeniería de Sistemas con mención en Gerencia de Sistemas de la Información

Autores

Br. Salinas Rodríguez, Michael Steve

Br. Valencia Moncada, Julio Andrés

Asesor:

Dr. Alberto Carlos Mendoza De Los Santos

Trujillo – Perú

2017

Resumen

En la presente investigación se analizaron y se evaluaron los niveles del riesgo que cuentan seis sedes de una entidad bancaria del Perú en el periodo de investigación de setiembre del 2016 a setiembre del 2017, así como la propuesta realizada sobre la implementación del sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2005 y las etapas del modelo Deming (Plan-Do-Check-Act) y que pueda ser aplicado, mantenido y auditado por la misma entidad, el cual garantiza que se logren los objetivos de la herramienta de seguridad y beneficiar a la empresa en la protección de sus activos, el cual permitirá el cumplimiento de las normas de manera eficiente para la protección de los activos de información.

Para lo cual, la metodología de investigación utilizada fue la de un diseño descriptivo puesto que nos enfocamos en el uso de cuadros y gráficos estadísticos por toda la información recopilada en los usuarios del banco intervinientes en los procesos seleccionados de la investigación.

Investigación que cuenta con resultados favorables para el diseño puesto que con la propuesta de la herramienta de seguridad se encontraron niveles de riesgos medios y altos (72% de riesgos en las áreas de estudio) que son los ideales para realizar la implementación de un sistema de gestión de seguridad de la información en las áreas de Seguridad, Usuarios de banca, TI, Sistemas, Helpdesk, observando en algunos casos que no cuentan con capacitaciones en seguridad de información, con los hallazgos obtenidos se demostró a la Alta Gerencia que el análisis y la evaluación de los riesgos deben ser mitigados o transferidos a un tercero de ser el caso estableciendo políticas de seguridad. En la fase de ejecución del sistema de gestión de seguridad de la información la alta gerencia debe poner mucho énfasis para que la herramienta de seguridad pueda mantenerse y ser monitoreada por especialistas en seguridad con el fin de preservar la confidencialidad, disponibilidad e integridad de los activos.

Estos activos se encuentran dentro de la propuesta, pues su fin es mejorar la seguridad en los procesos seleccionados de la entidad bancaria ya que se consideró que son los procesos más importantes en la entidad bancaria, del cual se realizó la propuesta en 6 de sus sedes principales y se demostró que es factible la propuesta para tomar acciones sobre la implementación en los procesos y que la entidad bancaria esté al nivel que las demás organizaciones se encuentran con esta herramienta ya implementada.

Palabras clave: Sistema de gestión de seguridad de la información, política de seguridad, activos, disponibilidad, confidencialidad, integridad, riesgos de información.

Abstract

In the present investigation, the risk levels of six agencies of a bank in Peru of the research period from september 2016 to september 2017, were analyzed and evaluated, as well as the proposal made on the implementation of the information security management system under ISO / IEC 27001: 2005 And the stages of the Deming (Plan-Do-Check-Act) model that can be applied, maintained and audited by the same entity, which guarantees that the objectives of the safety tool are achieved and benefit the company in the protection Of its assets, which will enable compliance with the rules in an efficient manner for the protection of assets.

For this, the research methodology used was that of a descriptive design since we focused on the use of tables and statistical graphs for all the information collected in the users of the bank involved in the selected processes of the investigation.

The research that has favorable results for the design since with the proposal of the security tool were found high risk levels (72% of risks in the study areas) that are the ideal ones to realize the implementation of the information security management system in the areas of Security, Banking users, IT, System and Helpdesk, noting in some cases that they do not have training in information security, with the findings obtained it was demonstrated to the High Direction that the analysis and evaluation of the risks should be mitigated or transferred to a third party, if necessary by establishing security polices. In the execution phase of the information security management system, High Direction must put a lot of emphasis so that the security tool can be maintained and monitored by security specialists in order to preserve the confidentiality, availability and integrity of the assets.

These assets are within the proposal, as their purpose is to improve security in the selected processes of the bank as it was considered to be the most important processes in the bank, from which the proposal was made in 6 of its agencies And it was demonstrated that it is feasible the proposal to take actions on the implementation in the processes and that the bank is at the level that the other organizations are with this tool already implemented.

Key words: Security policy, assets, availability, confidentiality, integrity, information risks.

Dedicatoria

Michael Salinas Rodríguez

Han pasado muchos años de mi nacimiento y pocos de tu partida, desde que llegaste a mi vida me ofreciste lo mejor, trabajaste duro y sin importar lo cansado que estabas siempre tenías un tiempo para la familia enseñándonos valores que nos formaron como buenas personas y esa educación que me brindaste me formó para ser un buen profesional… Papá, mi ejemplo, dedicado a Luis Fernando Cabanillas Chinchayán.

Eres una mujer que simplemente me hace llenar de orgullo y admiración, no habrá manera de devolverte tanto que me has ofrecido desde que estuve en tus brazos. Esta tesis es una meta más que logro, por tu esfuerzo en hacerme profesional obtuve este estudio gracias a mi trabajo pero más aún fue gracias a ti, no sé en dónde me encontraría de no ser por tus ganas de sacarme adelante, por tu empeño, tu compañía y tu amor… mi madre, dedicado a Graciela Rodríguez Castro.

Julio Valencia Moncada

La mayor de las virtudes de un ser humano es el no rendirse jamás, luchar hasta que no te queden fuerzas o dar todo por amor, ese amor que solo emana de Dios. Gracias en primer lugar a Dios por darme las fuerzas necesarias para culminar este proyecto, sin ti nada de esto hubiese sido posible.

Mamá, papá, estas palabras van dedicadas hacia ustedes quienes me dieron el aliento para no rendirme y culminar el proceso que había empezado. Elena y Abraham, su ejemplo de lucha diaria me ayudó desde pequeño hasta hoy, y sé que en el mañana seguiré aprendiendo de ustedes, muchas gracias.

A mi familia que siempre estuvo en cada paso que daba, todos ellos ocupan un importante espacio en mi corazón y están presentes en buenos y malos momentos, en especial a mi hijo, que es mi principal motivación para salir adelante. Gracias hijo por darme las mayores alegrías del mundo y ahora este esfuerzo lo comparto contigo, ¡Te amo!.

Agradecimientos

Nuestro especial agradecimiento a los docentes, personas de gran sabiduría que estuvieron apoyándonos en estos meses para lograr el objetivo de la obtención del grado de magíster:

Dr. Alberto Mendoza De Los Santos, que desde un principio nos apoyó en el proceso de la tesis del cual hemos pulido los más minuciosos detalles que ahora se muestra como una investigación que hemos luchado por obtener bajo lineamientos establecidos por la seguridad de la información, gracias también por el tiempo que se ha tomado pues es lo más valioso que nos ha podido brindar.

Mg. Rómulo Lomparte Alvarado, que durante la realización de nuestro proyecto ha sido nuestra mano derecha en asesorías sobre la seguridad de la información, por el tiempo que se ha tomado en las reuniones y apoyarnos en mejorar desde la redacción hasta el diseño de esta investigación.

Estamos muy agradecidos por transmitirnos sus conocimientos y la dedicación que han tenido en el tiempo que se han tomado, puesto que hemos logrado cumplir los objetivos y culminar la investigación con éxito y obtener con mucho sacrificio este título de magíster.

Así mismo, un sincero agradecimiento al profesor Aldo Martín Esquivel Quiñe, quien gracias a sus observaciones, sus correcciones y lo estricto que fue en el módulo de tesis nos enseñó de una manera directa y clara sobre cómo se debe de estructurar y enfocarse una tesis nivel magíster por tanto es de agradecer lo riguroso que fue para llevar esta investigación a cumplir con las expectativas puestas por la universidad hacia un enfoque empresarial.

Tabla de contenidos

Índice de tablas, gráficos y figuras

I. INTRODUCCIÓN

I.1. Realidad problemática

La información es el activo más importante de toda organización, es el eje que lleva a la empresa al éxito o al fracaso. (Gutiérrez, 2003) Desde esta óptica, la información se convierte en lo más fundamental para una empresa, sobre todo aquellas que trabajan con información financiera como es el caso de los bancos. En este tipo de organizaciones, la relevancia del riesgo es más notorio, pues los bancos trabajan con valiosa información que contienen datos y cartera de clientes, reportes de entrega de productos, ventas telefónicas, gestiones de cobranzas, portafolios de empresas, etc. Usualmente esta información es resguardada en espacios de archivos físicos y equipos de almacenamiento digital (Peinado, 2011).

Áreas clave de los bancos, son sus centros de contacto, sus sedes principales y sus agencias de atención al cliente, donde reciben y transmiten una gran cantidad de información acerca de consultas, reclamos, ventas y cobranzas, a través del uso de canales como: correos electrónicos, teléfono, servicios móviles y comunicaciones *online*, generando información valiosa de clientes y empresas asociadas a la entidad bancaria. Estas sedes cuentan con áreas donde existe un riesgo constante de pérdida o fuga de información debido a que se encuentra expuesta frente a otros usuarios como también a personal de empresas proveedoras, ya sea en ambientes controlados o no controlados, ocasionando la pérdida de la información, puesto que son sitios vulnerables el cual requieren de un sistema de gestión de seguridad de la información para minimizar los riesgos existentes y mantener la continuidad del negocio.

¿Y qué es un Sistema de Gestión de Seguridad de la Información?, pues es un conjunto de políticas y procesos para gestionar eficientemente la información, asegurando su confidencialidad, disponibilidad e integridad de los activos de información. Su propósito es asegurar que los riesgos de la seguridad de la información asumidos, gestionados, controlados y minimizados por la organización a través de procedimientos documentados y estructurados, permitiendo adaptarse a los cambios que se produzcan en el paso del tiempo, este riesgo de la seguridad de la información es el potencial de que una amenaza afecte o explote las vulnerabilidades de un activo causando pérdidas y daño en la organización.

Estos daños o pérdidas de información se producen por caída de servicios, interrupción en los dispositivos de red, falta de mantenimiento lógico o físico de los equipos, continuo uso de equipos o licencias antiguas, desastres naturales y siniestros, así como modificado, adulterado o sustraído por personal de la empresa, personal proveedor o personal sin autorización, aumentando los riesgos en la información, además que se encuentran expuestos frente a amenazas externas, como son los ataques informáticos o la ingeniería social, debido a que son blancos fáciles para los delincuentes informáticos o *hackers* si no tienen implementado medidas de seguridad para mitigar este tipo de ataques (Golovanov, 2015) (Santillán, 2009).

Las sedes de las entidades bancarias (principales, centros de contacto, agencias) que no cuentan con procedimientos, controles o políticas documentadas establecidas están expuestos a riesgos cada vez mayores, para ello, el Sistema de Gestión de Seguridad de la Información se apoya en distintos métodos o herramientas tales como ISO 27000, RISK IT, COBIT, ITIL, etc., el cual establecen reglas y estándares que sirven como guía para minimizar el impacto en caso de cualquier amenaza. Una de las normas en las que se apoya el Sistema de Gestión de Seguridad de la Información es la ISO27001, en las versiones 2005 y 2013, los controles que presenta esta norma son los adecuados para la gestión de la seguridad de la información en las sedes de las entidades bancarias, como también para diferentes tipos de empresas, donde se aplican los procesos de evaluación de riesgos de seguridad de información así como los propietarios de los riesgos (ISO 27001:2013, Cláusula 6.1.2) permitiendo así la continuidad de los procesos del negocio.

Estos procesos están documentados y almacenados en las áreas de Gerencias, Tecnologías de Información o Sistemas, esta última normalmente son de soporte y/o apoyo, directo a usuarios y procesos de la organización que generan el flujo de la información en el desarrollo de sus actividades para mantener la continuidad del negocio de los usuarios, estas áreas solo cuentan con una implementación de seguridad y mecanismos de control a nivel de aplicación para salvaguardar su información (Bertolín, 2008). El tener implementado un Sistema de Gestión de Seguridad de la Información permite conservar la confidencialidad, integridad y disponibilidad de la información, minimizar los riesgos y garantizar a las partes interesadas que estos serán manejados adecuadamente para asegurar la

disminución de los riesgos y adoptar las recomendaciones para proteger la información (ISO 27001:2013).

De esta manera, para asegurar la información frente a los riesgos existentes en las sedes de las entidades bancarias, las áreas responsables (Gerencias, TI, Sistemas, etc.) actúan reactivamente en respuesta frente a los incidentes en los procesos del negocio y problemas relacionados con la seguridad de la información. Estos incidentes, como los fraudes de dinero, robo de información, caída de servicios, etc., causan pérdidas económicas no solo a las sucursales de cada entidad bancaria sino a toda la empresa en mención pues según las recomendaciones que se redactan en los informes mensuales, destinados al área de Tecnologías de Información y gerencias, solo tratan de dar acciones correctivas mas no preventivas frente a estos incidentes que se presentan en sus locales o sedes, en la cual permite mitigar este tipo de incidentes para asegurar la información de manera temporal.

Tal es el caso que estos incidentes se minimizaron para el Banco Central de Reserva del Perú, pues es la única entidad bancaria a nivel nacional y el primer banco central en Latinoamérica que cuenta con un sistema de gestión de seguridad de información certificado con el IEC/ISO 27001:2013, con una validez desde junio del 2015 a junio del 2018, teniendo un beneficio sobre sus actividades para una mejora continua en los controles de sus procesos críticos (BCRP, 2015), este sistema ya implementado los pone un pie adelante frente a las demás entidades bancarias, pues el contar con esta herramienta de seguridad les permitirá a toda entidad bancaria asegurar todas sus gestiones, procesos y personal y tener un control adecuado contra amenazas que afecten la organización.

Por tanto, frente al estudio realizado, la información obtenida y el diseño propuesto en seis sedes de una entidad bancaria, el sistema de gestión de seguridad de la información nos brindó un conjunto de acciones sobre como planificar, gestionar, implementar controles e identificar los activos de la organización, definir su impacto, mantener actualizada la documentación de estos controles, políticas de seguridad y aplicar mejoras continuas para una mejor toma de decisiones de las seis sedes de la entidad bancaria y así mantener asegurada la información como la confianza con los clientes en las acciones que se realicen en los procesos del negocio.

I.2. Pregunta de investigación

¿De qué manera un Sistema de Gestión de Seguridad de la Información cuantifica en el riesgo de la seguridad de información en seis sedes de una entidad bancaria del Perú?

I.3. Objetivos de la investigación

A. Objetivo General

- Determinar la manera cómo un Sistema de Gestión de Seguridad de la Información cuantifica los riesgos de la seguridad de la información en seis sedes de una entidad bancaria del Perú.

B. Objetivos Específicos

- Diseñar un Sistema de Gestión de Seguridad de la Información en seis sedes de una entidad bancaria del Perú.
- Evaluar el proceso de gestión de riesgos en seis sedes de una entidad bancaria del Perú.
- Identificar las brechas existentes de seguridad para conocer el porcentaje de cumplimiento de los procesos y el impacto en los riesgos de seguridad de la información en las seis sedes de una entidad bancaria del Perú.
- Seleccionar los controles y objetivos de control de la seguridad de la información en las seis sedes de una entidad bancaria del Perú.

I.4. Justificación de la Investigación

En nuestra investigación se propone cuantificar los riesgos existentes en las seis sedes de una entidad bancaria a través de un sistema de gestión de seguridad de la información (SGSI) basados en la norma ISO27001:2005, su desarrollo brindará los procedimientos y lineamientos necesarios para identificar, tasar y evaluar los riesgos de la información y así documentar los controles necesarios que permiten proteger los procesos en seis sedes de una entidad bancaria del Perú, alineando de esta manera a los objetivos estratégicos establecidos en el *CORE* del negocio de la organización, como también en la reducción de gastos, puesto que hablar seguridad es hablar de inversión.

Con los resultados obtenidos por la cuantificación de los riesgos y del impacto del Sistema de Gestión de Seguridad de Información en las seis sedes de una entidad bancaria del Perú, estas tendrán una mejor imagen institucional (frente a las empresas competidoras, clientes o usuarios) permitiéndoles ingresar a los mercados internacionales.

I.5. Alcance de la investigación

Ante la realidad problemática descrita anteriormente, la realización de este proyecto es de diseñar una propuesta de cómo un Sistema de Gestión de Seguridad de la Información cuantifica los riesgos a los que la información está expuesta en seis sedes principales de una entidad bancaria del Perú, apoyándonos de otras herramientas que puedan construir un modelo acorde al negocio de la empresa, el cual permitirá el estudio de los riesgos existentes y la evaluación en la disminución de los mismos dentro de las 6 sedes principales que son sus 3 centros de contacto, la sede de sistemas, la sede principal y la sede central.

En cuanto al desarrollo del proyecto se pretende diseñar y describir un modelo de seguridad como es el SGSI donde su construcción está basado en el apoyo de la norma ISO 27001:2005 (gestión de seguridad de información y gestión de riesgos). Para esto se utilizan fuentes de investigación, documentos y encuestas realizadas a personal del banco y terceros para la recolección de datos. Esta información recopilada será de ayuda para realizar el modelo de Deming, que describe cuatro pasos importantes: ***Plan***, para determinar el estudio de los datos y generar una planeación del diseño de la propuesta, ***Do***, el cual nos permite realizar la simulación de los datos en base al diseño que se genera en el paso anterior, ***Check***, nos ayuda a contrastar los datos obtenidos con respecto a los datos actuales y por ultimo ***Act***, que, bajo lo anteriormente estudiado, queda a cargo por la alta gerencia la toma de decisiones sobre los resultados obtenidos, el trabajo no dará informes ni instrumentos para la ejecución del último paso del modelo Deming.

Por tal motivo, la investigación se basa en una metodología cuantitativa-descriptiva, puesto que utilizamos datos técnicos, información de la entidad bancaria, encuestas, plasmados en gráficos estadísticos en su desarrollo.

MARCO TEÓRICO

I.6. Antecedentes

Un primer trabajo corresponde a Barrante, Hugo (2012), quien realizo: "*Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos*", señala que el sistema de gestión de seguridad de la información contempla las cuatro etapas de Deming para su correcta puesta en marcha. Este tipo de proyectos debe ser avalado por la alta dirección para su correcto funcionamiento ya que sin esto no se podrá realizar ningún tipo de mejora y mucho menos aplicación.

Adicionalmente a esto, Robin, Salcedo (2014), añade en el "*Plan de implementación del SGSI basado en la norma ISO 27001:2013*" que el sistema de gestión de seguridad de la información puede ser implementado por toda empresa, grande o pequeña, pero su correcta implementación va a determinarse mucho de los correctos procesos con los que cuente la empresa, es decir, por más que podamos implementar un SGSI y cada área de la empresa trabaja a su manera, sin apoyar el procedimiento real de seguridad de información, no se podrá contar con el éxito del proyecto. Es por eso que siempre se recomienda primero enfocarse en el proceso, definirlo y establecerlo como único para la empresa y luego de eso se podrá implementar de manera correcta el SGSI.

En un trabajo realizado por Villena Moisés (2006) titulado "*Sistema de gestión de seguridad de información para una entidad financiera*", menciona que las políticas y los procesos en las empresas deben de estar bien definidos para poder realizar un correcto SGSI, más aun si se trata de entidades financieras. Estas deben de estar debidamente documentadas y actualizadas constantemente debido a que cualquier cambio en los procedimientos afecta a su correcta implementación.

Otro antecedente es el que menciona Espinoza Hans (2013) en "*Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo*" donde menciona que los riesgos de la pérdida de la información en una empresa no deben pasar como ideas de que algún momento pueden pasar o no, estas no deben tomarse a la ligera, es por eso que estos deben ser evaluados y clasificados para armar un plan de acción que le permita a la empresa evadirlos,

minimizarlos o aceptarlos, y así asegurar la seguridad de la información sin conllevar a gastos exagerados o desmedidos.

Algo similar menciona Rayme Rubén (2007) en "*Gestión de seguridad de la información y los servicios críticos de las universidades*" donde declara que los riesgos con respecto a la seguridad de la información pueden ser tomados de diferentes maneras, dependiendo de cada empresa estas evaluarán el nivel de importancia de los riesgos en el tiempo con la información confidencial que manejan. Estos procedimientos de niveles de importancia deben estar debidamente documentados para garantizar los riesgos que asumirá la empresa.

Una idea interesante que propone Álvarez Luis (2005) en "*Seguridad en informática (Auditoría de Sistemas)*" es que las empresas deben de ser muy cuidadosas en la evaluación de los riesgos y amenazas que podrán tener en el tiempo con respecto a la información valiosa que manejan. Esta clasificación no debe convertirse en un gasto innecesario por tratar de salvaguardar información de poco valor que la empresa pueda asumir en perdida. Por otro lado se debe de evaluar también el mejor lugar para su custodia y tomar en cuenta las amenazas de dichos lugares. Con estas evaluaciones se puede llegar a un concreto para asegurar de manera adecuada la seguridad de la información.

Otro antecedente que nos presenta Perafán, John; Caicedo, Mildred (2014) en "Análisis de Riesgo de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca" ellos hablan de que los riesgos que pueden tener las empresas son diferentes unas con otras, aun si son del mismo rubro o incluso si son de la misma empresa pero con diferente sede. Debido a esto es que la empresa debe tener identificado, como estación, sus propios riesgos que puede asumir y asegurar controles de calidad que permitan el monitoreo constante de su información.

Doria, Andrés (2015) menciona también en "Diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional iso/iec 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de córdoba" que los riesgos pueden clasificarse en tres tipos, riesgo que pueden mitigarse, es decir que pueden disminuir la probabilidad que sucedan, riesgos que podemos asumirlos, es decir que podemos aceptarlos como perdidas, y por ultimo riesgos que podemos transferirlos a terceros, es decir que pueden dárselo a cualquier otra empresa que la resguarde por nosotros. Esta clasificación

debe ser evaluada por el negocio y valorizada según sus objetivos, justificando la elección de cada una para la implementación o no implementación de los controles de seguridad.

Un aporte importante para nosotros es el de Villafranca, Daniel; Sánchez Luis; Fernández Eduardo y Piattini Mario (2005) en "*La norma ISO/IEC 17799 como base para Gestionar la Seguridad de la Información*" donde mencionan que es importante saber que las normas ISO no da un sistema de gestión de seguridad de la información, sino un conjunto de controles que nos sirven como guía para su adecuada implantación, sea en el ámbito que sea, esta nos derivara a una revisión detallada de nuestra situación en cuanto a la seguridad de la información y así poder tomar acciones dependiendo de los resultados e indicadores.

Hablar de sistema de gestión de seguridad de la información es hablar de riesgos en la información, como indica Cadme, Christ y; Duque Diego (2011-2012) en "*Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos Italimentos CIA. LTDA*" en donde asevera que las empresas deben de dar importancia a prevenir riesgos más que a corregirlos, el error usual en una empresa es pensar que más se gastara en prevenirlos que en corregirlos sin darse cuenta que a lo largo del tiempo gastaran más apagando incendios que evitándolos. Esto pasa debido a una falta de información, un plan o de colaboradores con una instrucción adecuada.

Según Gómez, Luis y Andrés, Ana (2012) en "*Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. 2ª edición*", concluye que la protección de los datos nunca se dará de forma total, pero si se puede llegar a tener procedimientos documentados y estandarizados que nos permitan minimizar los riesgos, asumirlos o tercerizarlos. En este caso la aplicación del SGSI es la mejor opción para poder mapear los procedimientos que aseguren la información del negocio.

I.7. Bases Teóricas

Según Friedrich Hayek, el orden espontáneo es una teoría social constituida por la información o el conocimiento de tipo personal o práctico que tiene cada ser humano en circunstancias particulares de tiempo y lugar para su propio bienestar y que no tienen intenciones de crear un orden o políticas (Zanotti, 2009). Por tanto, el

orden constructivo, que es todo lo contrario, impone orden y políticas por un grupo de personas de un determinado pueblo, comunidad o grupo de naciones para un determinado fin de manera global. Este es el caso de nuestras bases teóricas, donde se investigó en bibliografías así como también en la web del ISO, un organismo internacional formado por 153 organizaciones que promueve el uso de estándares propietarios, industriales y comerciales a nivel mundial, en este caso la web del ISO para la norma ISO 27001.

A. Riesgo en la seguridad de la Información

A.1. Gestión de Riesgo:

(Project Management Institute, 2013) Define que es una combinación entre las actitudes de los interesados frente al riesgo y la exposición al riesgo estratégico de un determinado proceso, realizando un análisis del perfil de riesgo de los interesados a fin de clasificar y calificar el apetito y la tolerancia al riesgo de los interesados del proyecto.

La gestión de riesgo es un enfoque estructurado para estudiar la posibilidad de que ocurra o no un riesgo, por tanto, para evitar que ocurra el riesgo, se lleva a cabo actividades para evaluar, mitigar el riesgo y estrategias para manejar el riesgo, reducirlos o aceptarlos, de tal forma que las posibles pérdidas y la posibilidad que se haga presente el riesgo se minimicen. En resumen, la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Lo más resaltante que se ve en la gestión de riesgo es:

1. Amenazas

En toda organización, los activos están sujetos a diferentes tipos de amenazas. Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a los activos y a la empresa, como pérdida de información, de su privacidad o bien un fallo en los equipos físicos. En la tabla II.2.1 se muestra la clasificación de las amenazas.

La figura II.A.1 muestra las amenazas más comunes contra los sistemas de información que existen en las organizaciones.

Tabla II.2.1
Clasificación de las amenazas

Naturales	Instalaciones	Humanas
- Inundaciones - Tsunamis - Tornados - Huracanes - Sismos - Tormentas - Incendios	- Fuego - Explosión - Caída de energía - Daño de agua - Pérdida de acceso - Faltas mecánicas	- Huelgas - Epidemias - Materiales peligrosos - Problemas de transporte - Pérdida de personal
Tecnológicas	**Operacionales**	**Sociales**
- Virus - Hacking - Pérdida de datos - Fallas de hardware - Fallas de software - Fallas en la red - Fallas en comunicaciones	- Crisis financieras - Pérdida de suplidores - Falla en equipos - Aspectos regulatorios - Mala publicidad	- Motines - Protestas - Sabotaje - Vandalismo - Bombas - Violencia laboral - Terrorismo

Fuente: http://www.isotools.pe/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/
Elaboración Propia

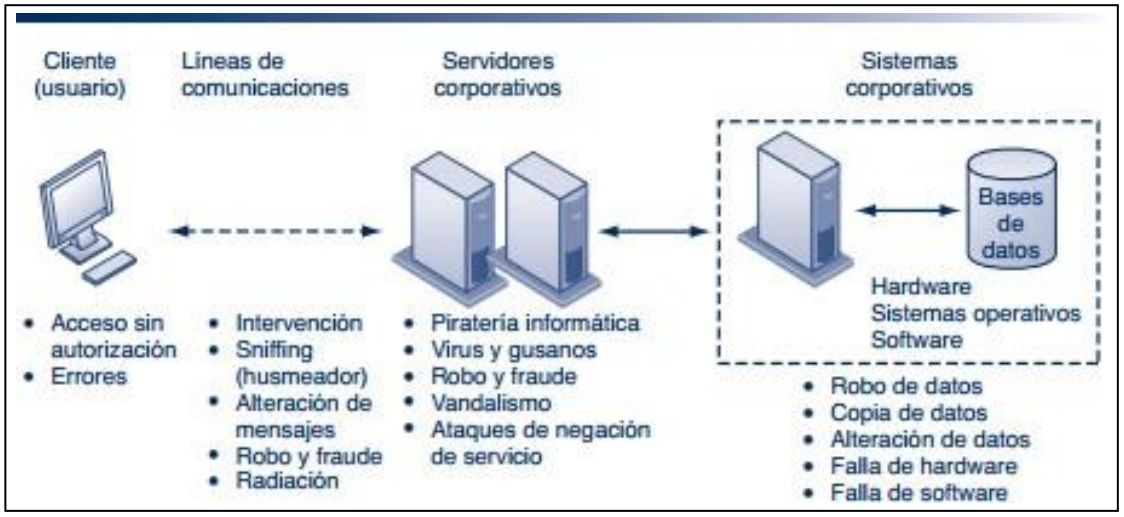


Figura II.A.1: Amenazas más comunes en las organizaciones
Fuente: Elaboración propia

2. Vulnerabilidades

Son las debilidades de seguridad asociadas con los activos de información de una organización, las vulnerabilidades también pueden clasificarse como se muestra en la tabla II.2.2.

"Es una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema" (Peltier, 2001).

"Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas" (Albert y Dorofee, 2003).

El tener almacenado gran cantidad de información de forma electrónica, estos son más vulnerables a todas las amenazas que se presentan, puesto que la interconexión de los ordenadores en una misma red permite que otros puedan tener acceso siempre y cuando no se haya activado el acceso seguro para el usuario autorizado, de no contar con acceso seguro se produciría un fraude, manipulación o abuso de la información, y al tratarse de entidades bancarias la adulteración de la información podría producir pérdidas económicas que afecten los procesos de la organización.

Otro caso es sobre las aplicaciones que se desarrollan a diario, alguno de ellos con malas intenciones con el fin de robar las credenciales de los clientes de bancos, tal es el caso que en diciembre del 2009 Google extrajo docenas de aplicaciones de banca móvil de su Android Market puesto que fueron actualizados para robar datos bancarios de clientes.

Tabla II.2.2
Clasificación de las vulnerabilidades

Seguridad física y ambiental	Control de acceso
- Control de acceso físico inadecuado a los ambientes - Ubicación en áreas sujetas a inundaciones - Almacenes desprotegidos - Carencia de programas para sustituir equipos - Mal cuidado de equipos - Susceptibilidad de equipos a variaciones de voltaje	- Segregación inapropiada de redes - Falta de política sobre escritorio limpio - Falta de protección al equipo de comunicación móvil - Política incorrecta para control de acceso - Password sin modificarse

Seguridad de los recursos humanos	
- Falta de entrenamiento en seguridad - Carencia de toma de conciencia en seguridad - Falta de mecanismos de monitoreo - Falta de políticas para el uso correcto de las telecomunicaciones - No eliminar los accesos al término del contrato de trabajo - Carencia de procedimiento que asegure la entrega de activos al término del contrato - Empleados desmotivados	
Mantenimiento y desarrollo de sistemas de información	**Gestión de operaciones y comunicación**
- Protección inapropiada de llaves criptográficas - Políticas incompletas para uso de criptografía - Carencia de validación de datos procesados - Carencia de ensayos de software - Documentación pobre de software - Mala selección de ensayos de datos	- Complicadas interfaces para usuarios - Control de cambio inadecuado - Gestión de red inadecuada - Carencia de mecanismos que aseguren el envío y recepción de mensajes - Carencia de tareas segregadas - Carencia de control de copiado - Falta de protección en redes públicas de conexión

Fuente: http://www.isotools.pe/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/
Elaboración Propia

3. Riesgos

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo de información de la organización. El nivel del riesgo depende de la vulnerabilidad y del impacto. El proceso de identificación y evaluación de riesgos y el de clasificación de activos permite determinar qué tan expuestos se encuentran los activos de información ante los ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización. Existen muchas clasificaciones para tipificar los riesgos, una de ellas es la que aparece en ISACA.

- Riesgo inherente: existencia de un error material o significativo sin un control compensatorio.
- Riesgos de control: existencia de un error que no pueda ser detectado por el sistema de controles establecido.
- Riesgos de detección: mal uso de procedimientos de detección de errores por parte de un auditor, que lleven a indicar que no existen errores en caso se encuentre alguno.

- Riesgos de negocio.
- Otros riesgos generales propios de la naturaleza de la auditoría

4. Controles

Son políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza en el logro de objetivos del negocio. Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es la presentada por ISACA.

- Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.
- Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones.

A.2. Identificación de los activos

El activo es todo lo que le da valor a la organización y puede considerarse como activos a las impresoras, dispositivos de almacenamiento (discos duros externos, etc.) aplicaciones, inclusive los mismos colaboradores de una empresa por poseer información en formato digital o físico, para identificarlos es necesario dimensionarlos en los 3 pilares de la seguridad que es la confidencialidad, disponibilidad e integridad, la figura II.A.2 muestra un ejemplo de algunos activos en una empresa.

Por otro lado, existen elementos que no son considerados activos puesto que no cuentan con información pero se relacionan directamente con los activos cercanos a él, por ejemplo, un sistema de aire acondicionado, no tiene información pero su función es mantener a los servidores a una temperatura adecuada para que no se sobrecalienten ni presenten fallas en su funcionamiento puesto que cuentan con información para la

organización. Otro punto importante son los activos que se relacionan directamente y la falla de uno repercute en otro, por ejemplo, una aplicación que la organización ha desarrollado para sus colaboradores, esta aplicación se almacena en un servidor y en caso el servidor falle pues también ocurrirá lo mismo en la aplicación y el impacto será alto en todos los colaboradores que lo estén usando.

Figura II.A.2 - Activos de información en una empresa

Fuente:http://www.isotools.pe/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/

A.3. Identificación de amenazas y vulnerabilidades

Como en toda organización, sus activos están expuestos a amenazas y que aprovechan de las vulnerabilidades para causar un impacto negativo adulterando su información y generar riesgos. Por tanto, es recomendable que se identifiquen qué amenazas y vulnerabilidades son las que están presentes en la organización por cada tipo de activo y realizar el análisis para posteriormente calcular el nivel de riesgo existente.

A.4. Cálculo del nivel de riesgo

Para calcular el nivel del riesgo se tienen metodologías como Margerit, ISO27001, Cramm, Octave, etc., cada una de ellas se diferencian por su fórmula de calcular el nivel del riesgo, en otros casos se considera la valorización del activo basado en su confidencialidad, disponibilidad e integridad tal cual lo indica la norma ISO 27001

Una de las fórmulas típicas es el impacto por la probabilidad de ocurrencia de que la amenaza atente contra el activo, el resultado se puede medir en valores numéricos o porcentuales, según se muestra en la figura II.A.3 los niveles de riesgo obtenidos mostrarán si existen riesgos que sean transferidos, aceptados o eliminados por la organización

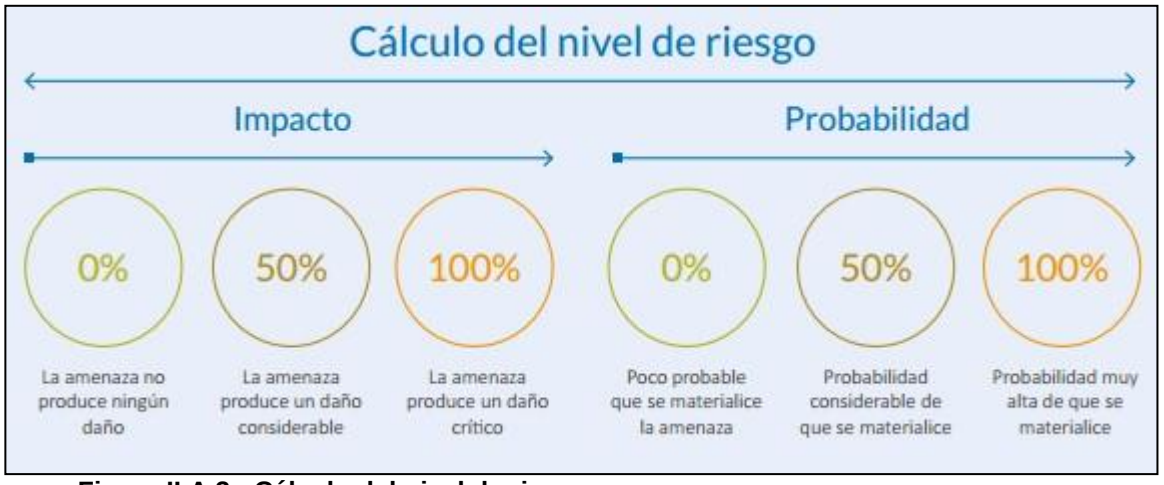


Figura II.A.3 - Cálculo del nivel de riesgo
Fuente: http://www.isotools.pe/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/

A.5. Evaluación del riesgo

(Laudon, 2012) Define que la evaluación del riesgo determina el nivel de riesgo existente en la organización, lo cual permite controlar las actividades o procesos específicos de manera apropiada. No todos los riesgos pueden anticipar o medir, pero la mayoría de las empresas podrán adquirir o aceptar qué riesgos existen dentro de sus áreas y a los que se enfrentan. Los gerentes de las organizaciones trabajan con oficiales de la seguridad de la información lo cual determinan el valor de los activos de información, los puntos de vulnerabilidad, la probable frecuencia de un problema y el potencial de daño.

El SGSI, en la evaluación de los riesgos, analiza el tratamiento que le debe dar a cada riesgo identificado. Una vez que conocemos los riesgos de la organización y dar el tratamiento a cada activo, se deben tomar en cuenta cuatro acciones fundamentales.

ACEPTAR EL RIESGO

La dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado puesto que la dirección conoce y acepta los riesgos. Los riesgos asumidos son controlados y revisados periódicamente y evitar que evolucionen y se conviertan en riesgos mayores.

MITIGAR EL RIESGO

Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

TRANSFERIR EL RIESGO

El riesgo que se presenta en un activo se da la responsabilidad a un tercero, para ello debe evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no solo coste económico sino también los riesgos que conlleva esta transferencia en cuando a la inclusión de un tercero.

ELIMINAR EL RIESGO

Suele resultar difícil para la empresa, por el tiempo, los responsables o por el costo, para conseguirlo, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

A.6. Establecimiento de los controles

En algunos casos el riesgo supera el nivel aceptable del riesgo luego de haber implementado los controles, por tanto, para ejecutar los controles de una manera adecuada y estructurada es necesario realizar un Plan de Tratamiento de Riesgos, el cual debe contener:

- Los responsables de implementar los controles

- Los recursos, materiales y herramientas a utilizarse en la implementación
- El plan de actividades
- Prioridad que se tiene por cada riesgo, empezando por los más críticos a los de baja criticidad.

A.7. Plan de gestión de riesgos

(Project Management Institute, 2013) Menciona que cuando se planifica la gestión de los riesgos es para definir de cómo vamos a realizar las actividades de los procesos en la gestión de riesgos de una actividad, proceso o proyecto. Tiene un beneficio importante de este proceso es que asegura que el nivel, el tipo y la visibilidad de la gestión de riesgos pues van a ser acordes tanto con los riesgos como con la importancia para la empresa. El plan de gestión de riesgos es vital para comunicarse y obtener el acuerdo y el apoyo de todos los interesados (personal de la empresa como proveedores) a fin de asegurar que el proceso de gestión de riesgos sea respaldado y llevado a cabo de manera eficaz a lo largo del ciclo de vida de la empresa

A.8. Medición del riesgo de seguridad de información

(IRAM, 2010) Menciona que la ISO 27001 requiere que los controles sean medibles, por tanto la ISO 27004 aporta la forma de llevar a cabo dichas mediciones, entonces, la operación de medición de la seguridad de la información comprende de actividades que son esenciales para asegurar que los resultados de las mediciones proporcionan información de un Sistema de Gestión de Seguridad de la Información, controles o políticas implementadas y la necesidad de acciones apropiadas de mejora, lo cual incluye la integración de los procedimientos de medición dentro de la operatividad del SGSI, así como también recolectar, almacenar y verificar los datos.

A.9. Ventajas de Seguridad de información frente a los RSI:

(IRAM, 2010) Según las ventajas que se tiene, menciona las siguientes:

- Facilitar la mejora de la efectividad de la seguridad de la información.
- Evaluar la efectividad del SGSI y su mejora continua.

- Lograr información objetiva y análisis para ayudar en la revisión de la gerencia, la toma de decisiones y justificar mejoras en los controles.
- Evaluar la efectividad de los controles de seguridad y los objetivos de control.

Bajo esas ventajas se encuentra un responsable cuya labora es garantizar con la implementación de políticas medidas y acciones, que contribuyan a la salvaguarda de la información del Organismo u oficina pública. Es importante que esta persona cuente con el aval y respeto de todas las direcciones del organismo, por esto a la hora de elegir a la persona que lleve adelante este rol es necesario que sea elegido en consenso.

B. Origen e historia de las normas ISO/IEC 27001

La Organización Internacional de estándares conocida como la ISO y la Comisión Electrotécnica Internacional por sus siglas IEC, son actualmente las principales organizaciones a nivel mundial para la estandarización de aspectos técnicos, de seguridad, entre otros. Dichas organizaciones, junto con otros organismos internacionales públicos o privados, participan en la realización de comités técnicos para establecer acuerdos y estándares en áreas específicas del conocimiento. Las normas conocidas como ISO/IEC 27001 y 27002, el cual su evolución se muestra en la figura II.B.1, que proporcionan un marco de gestión para la seguridad de la información aplicable por cualquier tipo de organización sin importar su naturaleza o tamaño, surgieron como resultado del Comité Técnico conjunto ISO/IEC JTC 1, llamado de las Tecnologías de la Información, subcomité 27 (SC 27), asociado con Técnicas de seguridad.

Estas normas se encuentran basadas en la antiguamente denominada norma BS 7799, elaborada por la BSI3 (Institución de estándares Británica) en 1995. La BSI publicó su norma 7799 en dos partes, la primera conocida como BS 7799-1, se elaboró como una guía de buenas prácticas de seguridad de la información y no se encontraba enmarcada en un sistema de seguridad de la información ni se encontraba diseñada para ser una norma certificable. Posteriormente en 1998, la BSI publicó la segunda parte de su norma, conocida como BS 7799-2, en la cual definió los requisitos que permitirían obtener una certificación del sistema de seguridad de la información (SGSI) por parte de una entidad independiente. Posteriormente, en el año 2000, la ISO adoptó la norma BS 7799-1 y la

denominó ISO 17799, sin cambios representativos respecto a su predecesora de la BSI, y fue hasta el año 2005 donde la ISO adoptó y publicó la norma BS 7799-2 bajo el nombre de ISO 27001, revisando al mismo tiempo la norma ISO 17799 y renombrándola posteriormente como ISO 27002 en el año 2007, la familia de estándares de esta norma 27001 se muestra en la tabla II.2.3. En su versión de 2005, la norma ISO 27001 contenía 11 dominios, cobijando 33 objetivos de control y 133 controles.

La norma ISO 27001, describe cómo gestionar la seguridad de la información en una empresa. Está determina como gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información (SGSI). La ISO 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar el SGSI, esta es la norma certificable por las empresas.

Figura II.B.1 - Evolución de la norma ISO 27000
Fuente: http://www.iso27001.es/iso27000.html

Tabla II.2.3
Familia de estándares ISO 27000

FAMILIA DE ESTANDARES ISO 27000		
ISO 27000 SGSI "Fundamentos y vocabulario"	ISO/IEC 27001:2005 Requerimientos	ISO/IEC 27002:2007 (ISO 17799:2005)
ISO/IEC 27003 "Lineamientos para la Implantación"	ISO/IEC 27004 Lineamiento "Métrica y ediciones"	ISO/IEC 27005 SGSI Lineamiento "Gestión del Riesgo"
ISO/IEC 27006 Requerimientos para entes que proveen auditoría y certificación a un SGSI	ISO/IEC 27007 Lineamientos para Auditar Sistemas de Seguridad de Información	ISO/IEC 27008 Lineamiento para Auditar Controles en Seguridad de Información

Fuente: http://www.iso27001.es/iso27000.html
Elaboración propia

C. Sistema de Gestión de Seguridad de la Información

C.1. Sistema de Información

(McLeod, 2000) Lo define como un conjunto de elementos que interactúan entre sí con el objetivo de apoyar los procesos o las actividades de una empresa, bien sea grande o pequeña. Además, un sistema de información no necesariamente se puede referir a equipos electrónicos (*hardware*), sino también a los documentos que están guardados físicamente en oficinas. Los elementos son de naturaleza diversa y normalmente incluyen el hardware necesario para que el sistema de información pueda operar, el recurso humano que interactúa con la información, alimentándose con datos o utilizando los resultados que genere. Tenemos también los datos, los programas ejecutados por las computadoras, las telecomunicaciones, políticas documentadas, etc.

C.2. Sistema de Gestión de Seguridad de la Información

(ISO27001, 2013) SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma pasando por un proceso y convirtiéndose en información, un ejemplo es el de la figura II.C.1, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

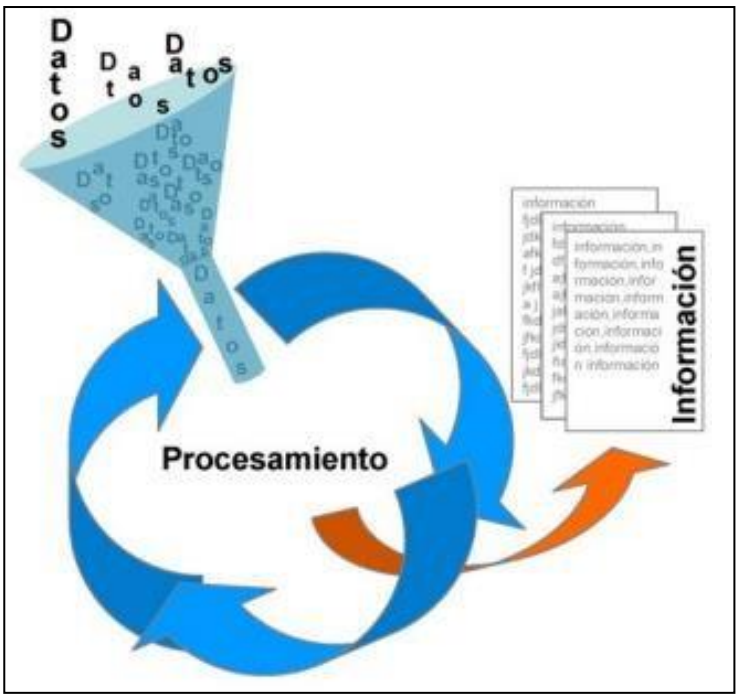


Figura II.C.1 - Procesamiento de la información
Fuente: http://www.iso27001.es/iso27000.html

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Estos riesgos guardan relación con las amenazas, activos, vulnerabilidades, controles tal como se muestra en la figura II.C.2.

Figura II.C.2 - Relación activos, riesgos, amenazas y vulnerabilidades
Fuente: http://www.iso27001.es/iso27000.html

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

En base al ciclo PDCA, el sistema de gestión de seguridad de la información cuenta con fases basadas en la norma ISO27001:

- Análisis y evaluación de riesgos.
- Implementación de controles.
- Definición de un plan de tratamiento de los riesgos o esquema de mejora.
- Alcance de la gestión
- Contexto de la organización
- Partes interesadas.
- Fijación y medición de objetivos.
- Proceso documental.
- Auditorías internas y externas.

C.3. Modelo Deming

(NTP-ISO27001, 2005) El modelo conocido como "Planear-Hacer-Verificar-Actuar" - PDCA (Plan-Do-Check-Act), por sus siglas en inglés, puede aplicarse a todos los procesos del SGSI. La Figura II.C.3 ilustra cómo un ISMS toma como entrada los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios genera productos de seguridad de la información (es decir: gestión de la seguridad de la información) que cumple estos requisitos y expectativas.

La adopción del modelo PDCA también reflejará los principios como se establecieron en la pautas de OECD (Guía para la Seguridad de los Sistemas de Información) para la gobernabilidad de los sistemas y redes de la seguridad de información. El ISO 27001:2005 provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación.

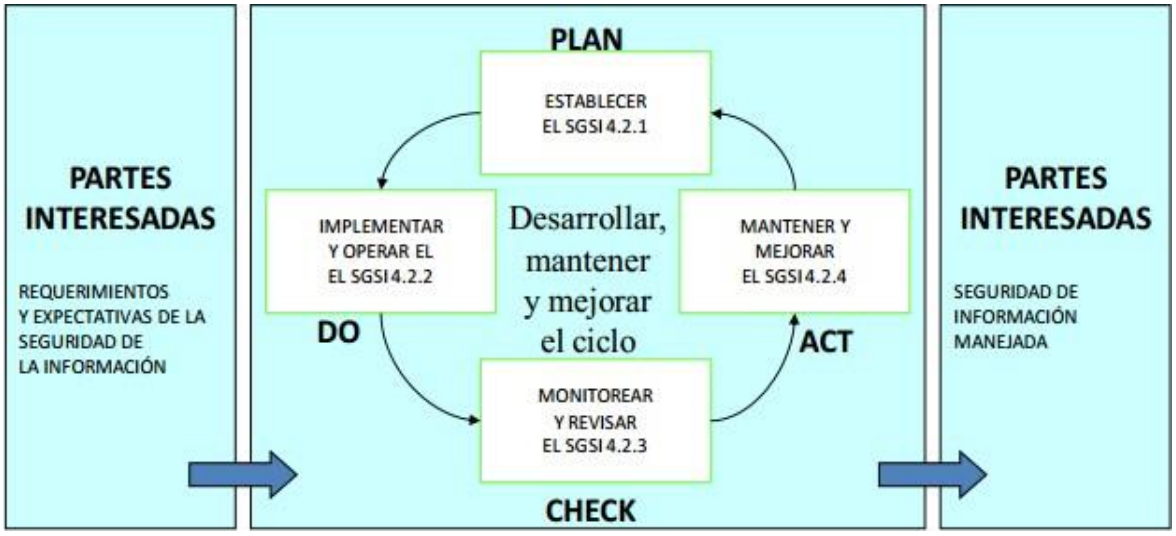


Figura II.C.3 - Modelo Deming
Fuente: http://www.iso27001.es/iso27000.html

1. Fase I: Plan - Establecer el SGSI

Establecer las políticas, objetivos, procesos y procedimientos de seguridad relevantes para administrar el riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos de la organización.

2. **Fase II: Do - Implementar y utilizar el SGSI**

   Implementar y operar las políticas, controles, procesos y procedimientos de seguridad.

3. **Fase III Check - Monitorizar y revisar el SGSI**

   Monitorear y evaluar el funcionamiento de los procesos con respecto a las políticas, objetivos y experiencia práctica de seguridad, informando sobre los resultados obtenidos a la gerencia para su revisión.

4. **Fase IV Act - Mantenimiento y auditoría del SGSI**

   Tomar acciones correctivas y preventivas basándose en los resultados de la revisión gerencial para alcanzar la mejora continua del SGSI.

C.4. Política de Seguridad

(Laudon, 2012) Menciona que consiste de procedimientos, actividades o enunciados que clasifican los riesgos de información, identifican los objetivos de seguridad que están implementados y que van acorde con la organización y sobre todo las herramientas a utilizar para lograr estos objetivos. La política de seguridad controla las políticas que determinan el uso eficiente de los recursos de información para que los usuarios o colaboradores lo usen de manera adecuada bajo la conformidad en el acceso por la gerencia.

D. Estudio de empresas internacionales certificadas en ISO 27001

El reporte anual de *ISO Survey of Management System Standard Certifications* (ISO MSSC) se encarga de realizar encuestas cada año sobre las certificaciones a sus estándares de sistemas de gestión mostrando el número de certificados válidos para los estándares de gestión ISO (ISO 9001, ISO 14001, ISO 27001) reportado para cada país. La encuesta ISO cuenta el número de certificados emitidos por los organismos de certificación que han sido acreditados por los miembros del Foro Internacional de Acreditación (IAF).

En la tabla II.2.4 se observa la evolución de las implementaciones del Sistema de gestión de seguridad de la información y el Top 10 de empresas que se han certificado en ISO 27001.

Tabla II.2.4
Top 10 de empresas que se han certificado en ISO 27001

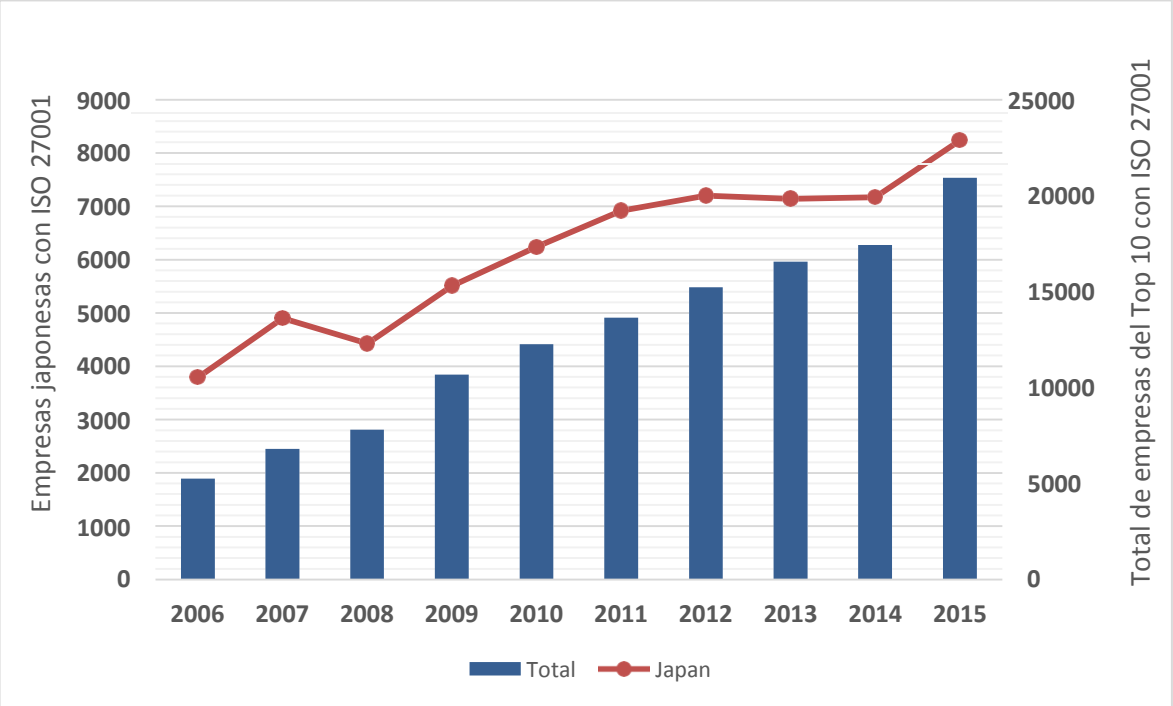
Country / Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Japan	3790	4896	4425	5508	6237	6914	7199	7140	7171	8240
United Kingdom	486	519	738	946	1157	1464	1701	1923	2253	2790
India	369	508	813	1240	1281	1427	1611	1931	2168	2490
China	75	146	236	459	509	664	790	965	1210	1469
United States of America	69	94	168	252	247	315	415	566	654	1247
Romania	4	16	44	303	350	575	866	840	893	1078
Italy	175	148	233	297	374	425	495	901	969	1013
Germany	95	135	239	253	357	424	488	581	634	994
Taipei, Chinese	159	256	702	934	1028	791	855	918	781	939
Spain	23	93	203	483	711	642	805	799	698	676
TOTAL	5245	6811	7801	10675	12251	13641	15225	16564	17431	20936

Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx

D.1. Análisis descriptivo de la relación entre el SGSI y la cantidad de empresas certificadas en ISO 27001

Como observamos en el gráfico II.1, en el periodo 2006 al 2015, la cantidad total de empresas en Japón y la cantidad de empresas del Top 10 por cada año guardan relación en cuanto al crecimiento por la certificación en ISO 27001, en Japón, entre los años 2011 al 2014 se evidencia que el crecimiento en la certificación ISO 27001 es corto, puesto que podría darse a entender por la cantidad de empresas jóvenes que cuentan con un tiempo corto en el mercado, aun así se evidencia que la certificación (mencionada anteriormente) lo consideran importante pues se sigue dando el crecimiento aunque en diferentes proporciones a lo que se muestra en los años 2006 al 2010.

Gráfico II.1
Crecimiento empresas japonesas con en ISO 27001 y Total empresas Top 10



Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx

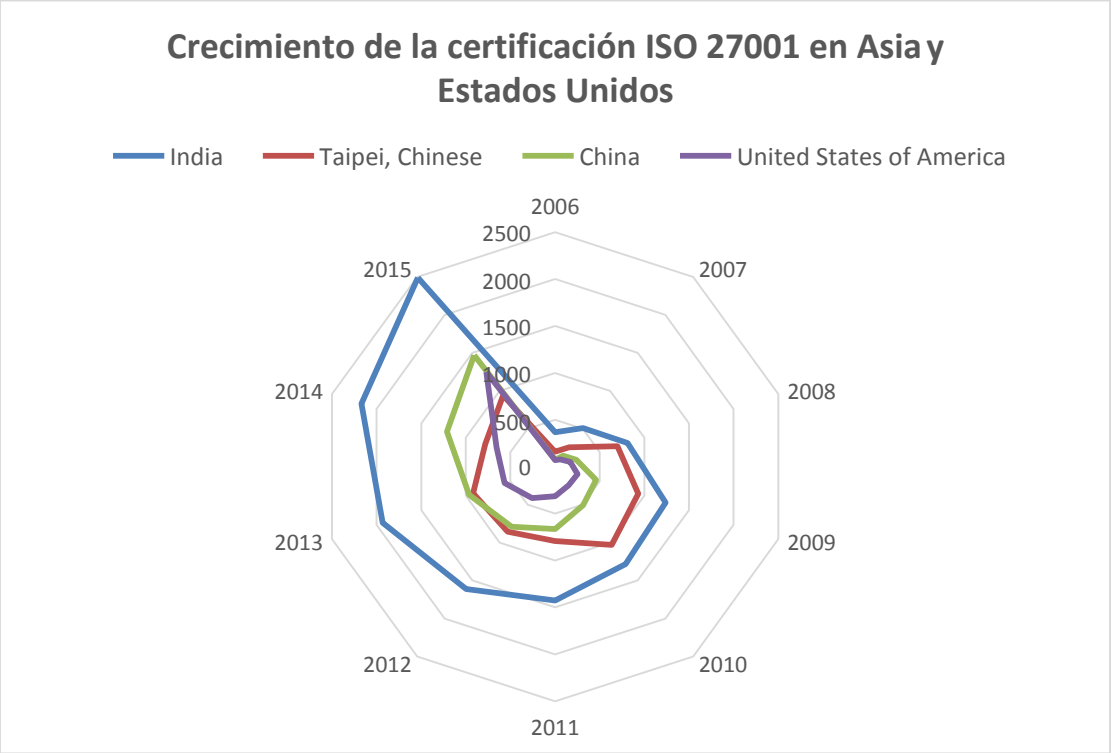
Elaboración propia

D.2. Análisis del crecimiento de la certificación ISO 27001 en las empresas del Top 10

Los gráficos siguientes corresponden a los datos sobre el crecimiento en la certificación ISO 27001 de las empresas de los países del Top 10 agrupados como Europa, Asia (considerando a Estados Unidos dentro del grupo asiático) y Japón por ser el país con el mayor número de empresas certificadas.

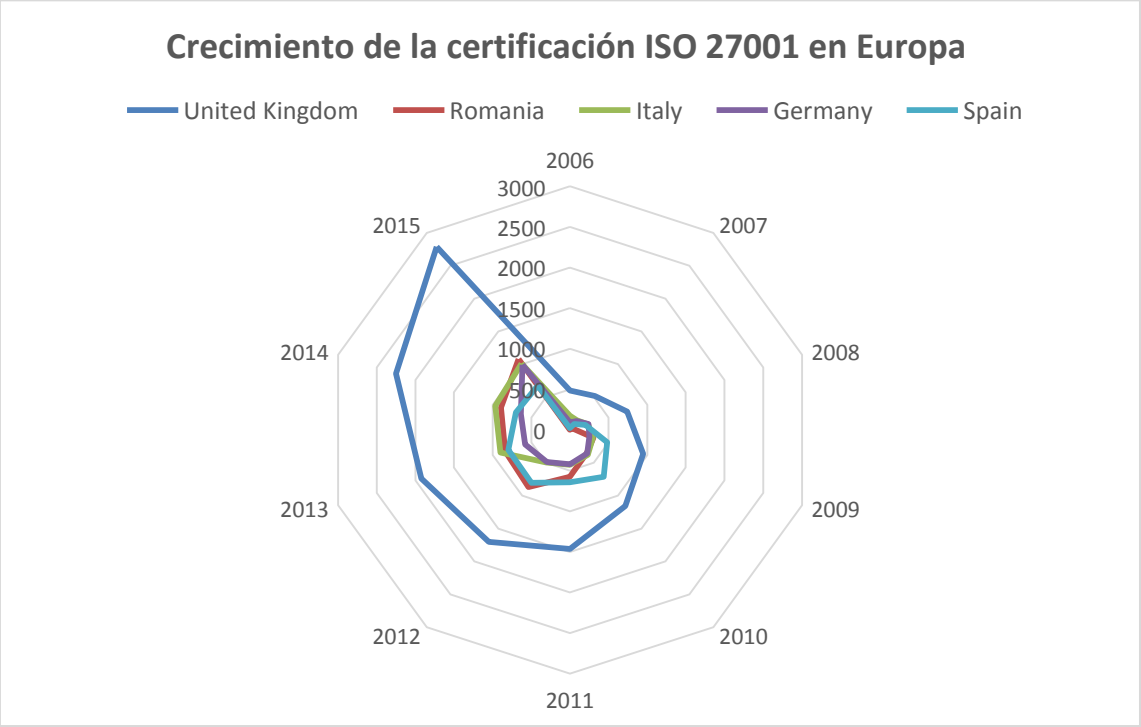
Lo que se destaca es que cada año se da un crecimiento notable en las empresas por contar con un SGSI y certificados con ISO 27001, así como también que Estados Unidos es el único país de América que está dentro del grupo Top 10, muy por encima de Brasil, Chile, Canadá y México. El Sistema de gestión de seguridad de la información debe ser el pilar de la seguridad en las empresas, por tanto las empresas deben tomar la decisión de implementarlo así como certificándose.

Gráfico II.2
Crecimiento de empresas de Asia y EEUU certificadas en ISO 27001



Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx
Elaboración propia

Gráfico II.3
Crecimiento de empresas de Europa certificadas en ISO 27001



Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx
Elaboración propia

D.3. Top 10 de empresas certificadas en ISO 27001 en Latinoamérica y Europa

Las siguientes tablas muestran el Top 10 de las empresas de los países en Latinoamérica y Europa certificados con ISO 27001.

Tabla II.2.5
Empresas de Latinoamérica certificadas en ISO 27001

Puesto	País	Certificaciones
1	Brasil	82
2	Colombia	81
3	México	80
4	Argentina	40
5	Chile	24
6	Costa Rica	10
7	**Perú**	**9**
8	Uruguay	8
9	Ecuador	5
10	República Dominicana	4

Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx

Tabla II.2.6
Empresas de Europa certificadas en ISO 27001

Puesto	País	Certificaciones
1	Reino Unido	1923
2	Italia	901
3	Rumanía	840
4	España	799
5	Alemania	581
6	República Checa	397
7	Países Bajos	316
8	Polonia	307
9	Hungría	280
10	Bulgaria	278

Fuente: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx

E. Seguridad Informática y la vulnerabilidad en los sistemas

La seguridad informática es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática e en realidad una rama de un término más genérico que es seguridad de la información, aunque en la práctica se suelen utilizar de distintas formas la aplicación de sus términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls y otras medidas que dependen del usuario. La figura II.E.1 muestra algunas amenazas en la red que existen o se pueden presentar en las organizaciones.

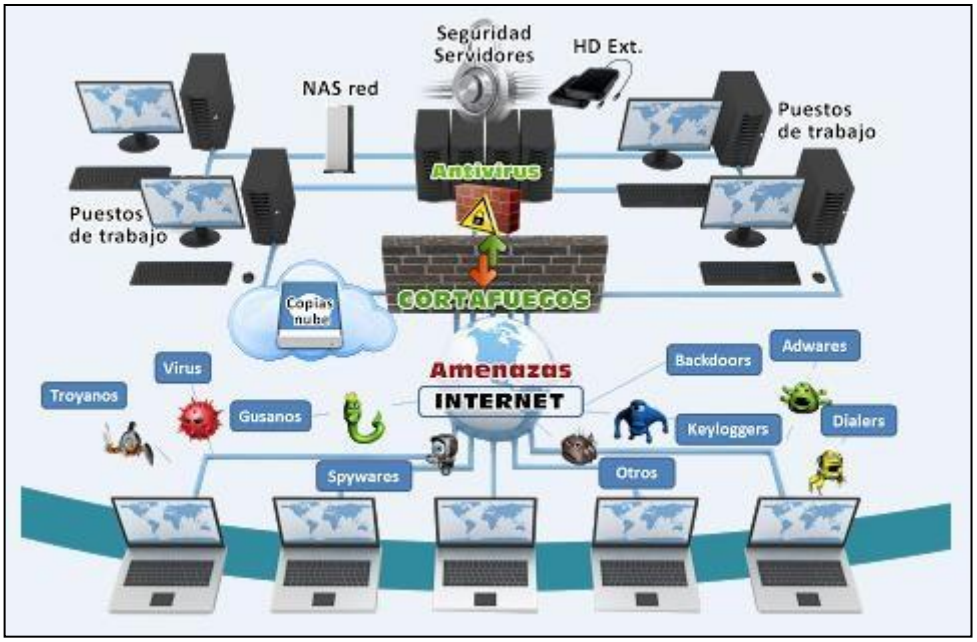


Figura II.E.1: Esquema de red Seguridad informática
Fuente: http://hakingmadrid.blogspot.pe/2013/09/certificaciones-de-seguridad

Cuando se almacenan grandes cantidades de datos en forma electrónica, estos son vulnerables a muchos más tipos de amenazas de los que existen en forma física. Los sistemas de información se interconectan en diversas ubicaciones a través de la red de la empresa. El potencial de acceso sin autorización, abuso o fraude no se limita a una sola ubicación sino que puede ocurrir en cualquier punto de la red de la empresa, para ello todo el personal debe contar con un

plan de capacitación en Cyberseguridad puesto que pueden provocar daños al introducir errores o acceder a los sistemas sin autorización como también abrir aplicativos o programas sin tener el conocimiento sobre su funcionamiento. Algunas de las amenazas en los sistemas de información son los siguientes:

E.1. Spoofing

Redirige un vínculo web a una dirección distinta de la que se tenía pensada, en donde el sitio web se hace pasar por el destino esperado. Al hacer esto el hacker recolecta la información a través de este sitio web falso.

E.2. Hackers

Son individuos que intentan obtener acceso sin autorización a un sistema computacional. En la comunidad de los hackers existe el Cracker, aquel que accede a los sistemas sin autorización con intención criminal, a menudo los hackers y los crackers aprovechan las diversas vulnerabilidades del sistema con el fin de obtener información y en algunos casos manipularla, así como los daños en los sistemas, robo de información, la interrupción de un sitio web, cibervandalismo, etc.

E.3. Sniffer

Es un tipo de programa espía que monitorea la información que viaja a través de una red. Cuando se utilizan de manera legítima, los *Sniffers* ayudan a identificar los puntos vulnerables en la red y la actividad que pasa a través de una red, cuando se utiliza de manera ilícita los *Sniffers* permiten al hacker robar la información de cualquier parte de la red, como mensajes de correo electrónico, archivos de la compañía, informes confidenciales, etc.

E.4. Ataque de negación de servicio

Este tipo de ataques es para inundar un servidor de red o de web con muchos miles de comunicaciones o solicitudes de servicios falsos para hacer que la red falle. La red recibe tantas solicitudes que no puede mantener el ritmo y por lo tanto no está disponible para dar servicio a las solicitudes legítimas.

E.5. Robo de identidad

Es un crimen en el que un impostor obtiene piezas clave de información personal, para hacerse pasar por alguien más. La información puede ser utilizada para obtener crédito, mercancía o servicios a nombre de la víctima, o para proveer al ladrón credenciales falsas.

I.8. Marco Conceptual

A. **Aceptación del riesgo:** Decisión de aceptar el riesgo que se está presentando.
B. **Activo:** Es todo lo que le da valor a la organización.
C. **Amenaza:** Es la posibilidad de ocurrencia de cualquier tipo o acción que puede causar daño a la organización.
D. **Análisis del riesgo:** Uso sistemático de información para identificar amenazas y estimar el riesgo.
E. **Ataques informáticos:** Es un método por el cual una persona, haciendo uso de sus sistemas informáticos, intenta tomar el control con el fin de dañar o perjudicar o vulnerar la red, los sistemas de la organización o de una persona en particular.
F. **Centro de contacto:** Es una oficina, espacio amplio de trabajo o empresa en la cual se encarga de recibir y transmitir una amplia cantidad de llamadas y pedidos a través del teléfono, brindando las atenciones en cuanto a consultas, ventas, etc.
G. **Cobit:** Marco de negocio para la gestión de la empresa, permitiendo el desarrollo de políticas, procedimientos para que la organización esté alineada con la tecnología de la información y lograr mejores resultados.
H. **Confidencialidad:** Es la información que se encuentra disponible exclusivamente para personas que cuentan con autorización.
I. **Continuidad del negocio:** Se refiere a prevenir, mitigar y recuperarse de una interrupción de los servicios o procesos de la empresa.
J. **Control:** Es un método para gestionar el riesgo que incluye las políticas, procedimientos, directrices y prácticas organizativas con el fin de mitigar la vulnerabilidad o el impacto en los activos de información.
K. **Declaración de aplicabilidad:** Es un documento importante, según la norma ISO27001:2005 cláusula 4.2.1, que contiene todos los objetivos de control y controles y que da las exigencias que deben seguirse para estar en conformidad.
L. **Disponibilidad:** Utilización de la información por personas autorizadas en el horario que lo requieran.

M. **Gestión de la seguridad:** Conjunto de actividades que incluye la administración de riesgos, el mantenimiento de políticas, clasificación de información y capacitación a los miembros de la organización.

N. **Gestión de la Seguridad de la información:** Conjunto de prácticas, procesos o procedimientos que se encarga de reducir las amenazas y riesgos del que información está expuesta.

O. **Gestión de riesgo:** Es un proceso que se encarga de la identificación, análisis y cuantificación de las de las probabilidades de ocurrencia de las amenazas, disminuir las vulnerabilidades y promover acciones de conservación de la información.

P. **Impacto:** Es la diferencia en las estimaciones del estado de seguridad del activo de información antes y después de la materialización de la amenaza sobre este.

Q. **Información:** Es el activo más importante que posee la organización, como también es un conjunto organizados de datos procesados, que constituyen un mensaje para el conocimiento del usuario.

R. **Ingeniería social:** Es el método de obtener información confidencial, es una técnica mediante engaños a los usuarios o administradores de la organización, empleada por investigadores o delincuentes informáticos.

S. **Integridad:** Mantenimiento de la información en cuanto a su contenido, protegiéndola de modificaciones o alteraciones no autorizadas manteniendo su validez.

T. **ISO:** International Organization for Standardization, es una federación mundial de organismos nacionales de normalización, alrededor de 160 países, trabajan a nivel de comités técnicos.

U. **ISO 27000:** Es un conjunto de estándares, en desarrollo o que están desarrollándose por ISO el cual brinda un marco de gestión de seguridad de la información destinado para todo tipo de organización.

V. **ISO 27001:** Es la certificación para las organizaciones. Especifica los requisitos para la implantación del SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

W. **ISO 27001:2005:** Norma que facilita la integración de los sistemas de gestión de riesgos en la seguridad de la información y activos utilizando el modelo Deming o PDCA.

X. **ISO 27001:2013:** Es la norma que facilita la integración de los sistemas de gestión donde los riesgos en la seguridad de la información deben ser abordados, documentados y disminuidos

Y. ITIL: Biblioteca de infraestructura de tecnologías de información, es un marco de trabajo de mejores prácticas del cual se encarga a mejorar y facilitar la entrega de servicios de tecnologías de información, logrando su calidad y eficiencia en las operaciones.

Z. Manual de seguridad: Es el documento que administra todo el sistema de seguridad de la organización, expone y determina los objetivos, el alcance, responsabilidades, políticas y directrices del SGSI.

AA. Modelo de Deming: Son las herramientas para lograr la mejora contínua en las organizaciones permitiendo la reducción de costos, optimizar la productividad, mayor participación en el mercado y aumentando la rentabilidad, etc.

BB. Objetivos de control: Declaraciones de resultados deseados o propósitos a lograr. Proveen los lineamientos necesarios para delinear las políticas de manera clara y los controles necesarios.

CC. Outsourcing: Proceso de contratación hacia una empresa externa para que se haga cargo de una parte de la actividad o la producción de la organización.

DD. Plan de tratamiento de riesgo: Son las actividades que se ejecutan una vez tomada la decisión relacionada con el tratamiento de riesgos, aquí es donde se determinan los recursos a utilizar, los entregables, cronogramas y la supervisión del avance y cumplimiento.

EE. Política y objetivos de seguridad: Documento que establece el compromiso de la gerencia y colaboradores de la organización en la gestión de la seguridad de la información.

FF. Procedimientos: Documentos que aseguran que se realicen de forma eficaz la planificación, operación, y control de procesos de seguridad de información.

GG. Riesgo: Probabilidad de que ocurra un desastre ante una amenaza interna o externa.

HH. Riesgo residual: Riesgo remanente después de un tratamiento de riesgo

II. Risk IT: Marco de negocio que establece prácticas con el fin de identificar, gobernar y administrar los riesgos asociados a la organización y la relación que existe con las tecnologías de la información.

JJ. Seguridad de la información: Es determinar qué es lo que necesita ser protegido y porqué, ante qué eventos debe ser protegido y como proteger la información.

KK. Sistema de gestión de seguridad de la información: Se encarga de preservar la confidencialidad, integridad y disponibilidad de la información en

las organizaciones, estableciendo políticas y controles en relación a los objetivos del negocio de la organización.

LL. Seguridad informática: Conjunto de medidas de control que buscan proteger la infraestructura tecnológica de información y comunicaciones que soportan los procesos de las empresas.

MM. Vulnerabilidad: Es una debilidad que se presenta en un sistema, aplicación, equipo de la infraestructura de la organización, proceso, en la cual puede ser explotada para violar o adulterar la integridad del activo.

II. HIPÓTESIS

II.1. Declaración de hipótesis

El Sistema de Gestión de Seguridad de la Información cuantifica los riesgos de la seguridad de la información en 6 sedes de una entidad bancaria del Perú.

II.2. Operacionalización de variables

A. Variable 1: Variable dependiente

Riesgo de la seguridad de la información

B. Variable 2: Variable Independiente

Sistema de Gestión de Seguridad de la Información

Tabla III.2.1
Operacionalización de la variable dependiente

Variable	Tipo de Variable	Operacionalización	Categoría o dimensiones	Definición	Indicador	Nivel de medición	Unidad de medida	Índice	Valor
Riesgo de seguridad de la información	Cuantitativa discreta	Es el potencial de que una amenaza afecte o explote las vulnerabilidades de un activo causando pérdidas y daño en la organización y afectando la seguridad de la información que la empresa tiene implementada.	Riesgo	Probabilidad de que ocurra un desastre ante una amenaza interna o externa	Cantidad de riesgos detectados en la organización	Nominal	Unidades	Índice de riesgos	Los riesgos existentes que existen en la organización
			Evaluación de riesgos	Es un proceso que se encarga de conocer el valor que el auditor le da a cada riesgo en cuanto a las amenazas, vulnerabilidades y activos en la organización.	Valores enteros de los resultados del cálculo del riesgo	Intervalos	Unidades	Índice de tablas y valores	Valores enteros que son analizados por el auditor y la gerencia
			Plan tratamiento de riesgos	Son las actividades a implementar, las decisiones a ejecutar cuando han sido aprobados por gerencia, estimando recursos, cronograma y responsabilidades	Cantidad de actividades que están bajo responsabilidad de todo el personal involucrado en la seguridad	Nominal	Unidades	Índice de actividades	Las actividades del plan se entregaron en el plazo establecido
			Brechas de seguridad	Son los orificios o las aberturas que se aprovechan de un falla o vulnerabilidad para producir un error en los procesos o sistemas	Cantidad de brechas existentes en la organización	Intervalos	Unidades	Índice de brechas	Todas las brechas analizadas y mitigadas por la herramienta de seguridad
			Amenaza	Es la posibilidad de ocurrencia de cualquier tipo o acción que puede causar daño a la organización	Cantidad de amenazas encontradas en la organización	Nominal	Unidades	índice de amenazas	Amenazas detectadas en la organización
			Vulnerabilidad	Es una debilidad que se presenta en un sistema, aplicación, equipo de la infraestructura de la organización, proceso, en la cual puede ser explotada para violar o adulterar la integridad del activo	Cantidad de vulnerabilidades encontradas en la organización	Nominal	Unidades	índice de vulnerabilidades	Vulnerabilidades detectadas en la organización

Fuente: Elaboración propia

Tabla III.2.2
Operacionalización de la variable independiente

Variable	Tipo de Variable	Operacionalización	Categoría o dimensiones	Definición	Indicador	Nivel de medición	Unidad de medida	Índice	Valor
Sistema de Gestión de seguridad de la información	Cuantitativa discreta	Conjunto de políticas y procesos documentados para gestionar eficientemente la información, asegurando su confidencialidad, disponibilidad e integridad de los activos y es asegurar que los riesgos de la seguridad de la información asumidos, gestionados, controlados y minimizados por la organización adaptarse a los cambios que se produzcan en el paso del tiempo	Confidencialidad	Es la información que se encuentra disponible exclusivamente para personas que cuentan con autorización	Cantidad de información según los acuerdos de confidencialidad por cada trabajador	Ordinal	Unidades	Índice de información confiable	Confidencialidad de la información presente en la organización
			Disponibilidad	Utilización de la información por personas autorizadas en el horario que lo requieran	Cantidad de información disponible por cada trabajador	Ordinal	Unidades	Índice de información disponible	Disponibilidad de la información presente en la organización
			Integridad	Mantenimiento de la información en cuanto a su contenido, protegiéndola de modificaciones o alteraciones no autorizadas manteniendo su validez	Cantidad de información íntegra por cada colaborador	Ordinal	Unidades	Índice de información íntegra	Integridad de la información presente en la organización
			Activo	Todo aquello que le da valor a la organización.	Cantidad de activos en la organización	Nominal	Unidades	índice de activos	Activos detectados en la organización por áreas y clasificados.
			Controles de seguridad	Son los métodos para gestionar los riesgos, que incluyen políticas, procedimientos, prácticas, directrices o estructuras organizativas	Cantidad de controles a implementar	Intervalos	Unidades	Índice de controles	Mantener y monitorear los controles que se implementarán
			Política de seguridad	Conjunto de normas y procedimientos para proteger los activos de la organización y regular el uso que tienen con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma	Cantidad de políticas a implementar	Intervalos	Unidades	Índice de políticas	Mantener y monitorear las políticas que se implementarán

Fuente: Elaboración propia

II.3. Propuesta de solución

A. Proceso de ejecución para implantar el SGSI mediante el ISO 27001:2005

De las propuestas realizadas a la organización en cuanto un sistema de seguridad fue del Sistema de gestión de seguridad de la información en sus normas y versiones ISO 27001:2005 e ISO 27001:2013 respectivamente, dando a conocer el desarrollo de cada uno en cuanto a las necesidades sobre el diseño de la seguridad de la información hasta los controles y auditorías que se deben aplicar luego de su implementación para todo tipo de organizaciones en cada una de sus versiones, los datos, información y documentación recopilada a través de las técnicas e instrumentos se trabajaron en base a tablas que evalúan el nivel de riesgo que presentan las seis sedes de una entidad bancaria, con un estudio más detallado frente a los controles y el costo que implica la implementación, desde el uso del modelo Deming en la versión 2005 y la aplicación y desarrollo de controles y objetivos de control como también presenta la versión 2013.

Empresas como Telefónica del Perú (Data Center, Outsourcing de TI, Disaster Recovery/Businnes Continuity), Hermes (Proceso de financiamiento en entrega), Indecopi, son algunas empresas en Perú que han obtenido la certificación ISO27001:2005 y mantienen su vigencia en los procesos mencionados, por otro lado, el Banco Central de Reserva del Perú es la única entidad bancaria que cuenta con una certificación ISO27001:2013 en el proceso “Transferencias Interbancarias del Sistema de Liquidación Bruta en Tiempo Real (Sistema LBTR)”, proceso del cual no está sujeto a los procesos tecnológicos a nivel usuario que se mencionan en el punto 3 (Alcance del SGSI) de la cláusula 2 del modelo Deming (Plan).

Entonces, por la información obtenida en cuanto a la versión 2005 se propuso a la organización el uso de la herramienta del Sistema de Gestión de Seguridad de la Información a través de su norma ISO 27001:2005, puesto que es el estándar que ha demostrado mayor madurez en Europa y Estados Unidos (Ver Gráfico II.2 Crecimiento de empresas de EEUU certificadas en ISO 27001 y Gráfico II.3 Crecimiento de empresas de Europa certificadas en ISO 27001) Cuadro Tabla II.2.5: Empresas de Latinoamérica certificadas en ISO 27001) como también la cantidad de empresas con las que Latinoamérica cuenta en la

certificación de esta norma (Ver Tabla II.2.5 Empresas de Latinoamérica certificadas en ISO 27001).

Esto es con el propósito de fomentar la cultura de la seguridad de la información para que de manera gradual hacer la transición a la versión de la norma más reciente que es la ISO 27001:2013. El proceso que se realizó en la propuesta del SGSI es a través de las actividades que nos brinda el ISO 27001:2005, mostrado en la figura III.A.1.

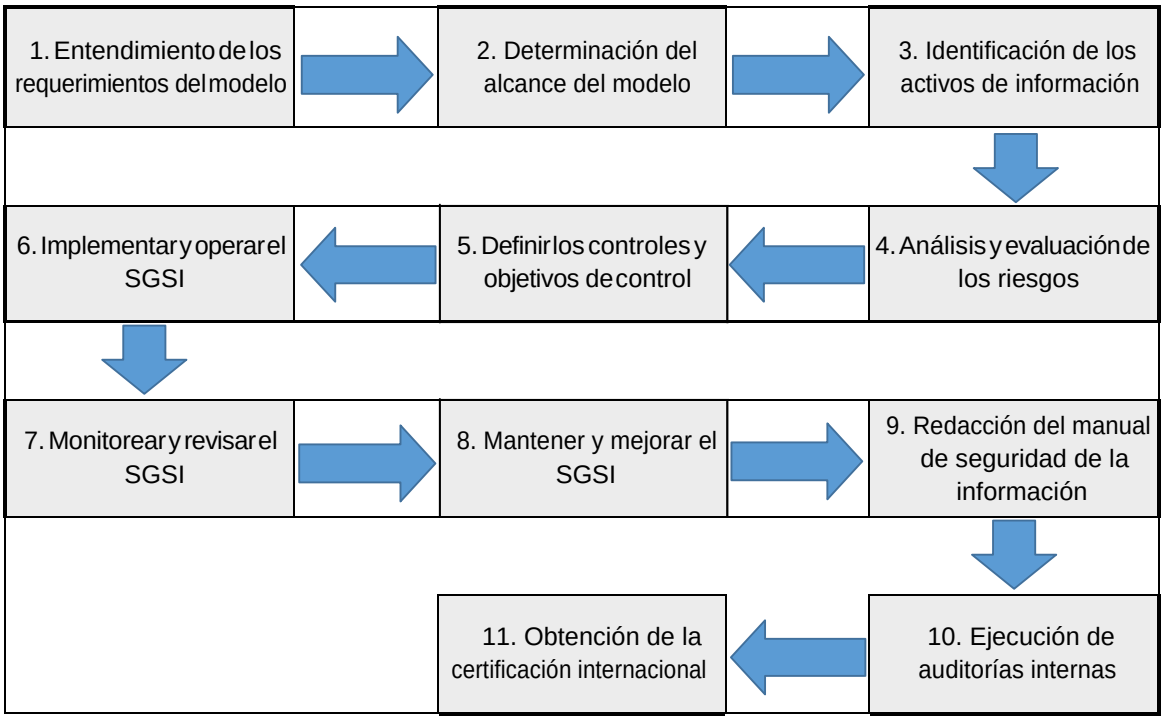


Figura III.A.1 - Proceso a ejecutar el SGSI basado en el ISO 27001:2005
Fuente: Elaboración propia

B. Operaciones o unidades que están involucradas en el proyecto

En los procesos seleccionados que se trabajó en la propuesta (Atención y solución de incidencias, Control de acceso al *datacenter* e Instalación de *software*) se está contando con toda el área y personal involucrado (Operaciones, Infraestructura de TI, Seguridad, Accesos, Helpdesk, Usuario de línea bancaria, Soporte y Sistemas). Las siguientes tablas muestran el detalle de las actividades a los que el Sistema de Gestión de seguridad de la información trabajará en conjunto con las áreas y el personal mencionado anteriormente.

Tabla III.3.1
Cronograma propuesta proyecto Seguridad de la información

Cronograma sobre la propuesta del proyecto de Seguridad de la Información																										
Actividades	**Horas**	**05/06/17 - 09/06/17**					**12/06/17 - 16/06/17**					**19/06/17 - 23/06/17**					**26/06/17 - 30/06/17**					**03/07/17 - 07/07/17**				
		Semana 1					**Semana 2**					**Semana 3**					**Semana 4**					**Semana 5**				
		L	**M**	**Mie**	**J**	**V**	**L**	**M**	**Mie**	**J**	**V**	**L**	**M**	**Mie**	**J**	**V**	**L**	**M**	**Mie**	**J**	**V**	**L**	**M**	**Mie**	**J**	**V**
1. Entendimiento de los requerimientos de la empresa Entrevista con la Alta gerencia	4																									
2. Estudio y determinación del alcance del modelo	6																									
3. Identificación de los activos de información en las 6 sedes principales de la entidad bancaria	60																									
4. Análisis y evaluación de los riesgos identificados	84																									
5. Definir los controles y objetivos de control por cada activo, amenaza y riesgo.	21																									
6. Discusión de la propuesta para la implementación del SGSI por la Alta Gerencia y áreas involucradas	12																									
7. Aprobación por la gerencia en la implementación del SGSI	3																									

Fuente: Elaboración propia

Tabla III.3.2
Cronograma propuesta Implementación proyecto SGSI

Cronograma de actividades para la implementación del proyecto de Seguridad de la Información																								
Actividades	Horas	31/07/17 - 27/10/17				30/10/17 - 24/11/17				27/11/17 - 22/12/17				08/01/18 - 02/02/17				05/02/18 - 02/03/18				05/03/18 - 09/03/18			
		Mes				Semanas				Semanas				Semanas				Semanas				Semana Final			
		Jul.	Ago.	Set.	Oct.	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	L	M	Mie	J
1. Implementar y operar el Sistema de Gestión de Seguridad de Información	1020																								
2. Monitorear y revisar el Sistema de Gestión de Seguridad de Información	90																								
3. Mantener y mejorar el Sistema de Gestión de Seguridad de Información	60																								
4. Redacción del manual de seguridad de la información	45																								
5. Ejecución de auditorías internas o externas.	30																								
6. Entrega y revisión del informe final del SGSI bajo la norma ISO27001:2005	3																								
7. Obtención de la certificación internacional ISO 27001:2005	10																								
8. Discusión de los resultados sobre el SGSI implementado	4																								

Fuente: Elaboración propia

C. Los recursos y costos asociados

Los recursos y costos asociados en el proyecto ascienden a los 200082 dólares americanos, tal como se mencionan en la tabla V.2.8.

D. Las normas de cumplimiento obligatorio

Una de las normas que promueve una buena implementación del Sistema de gestión de seguridad de información es el ISO 27001 en su versión 2005.

El ISO27000 básicamente contiene una visión general de las normas de la serie y un conjunto de definiciones y términos necesarios para comprender y aplicar la serie.

El ISO 27001 sustituye a la ISO 17799-1, donde abarca un conjunto de normas relacionadas con la seguridad informática. Se apoya en la norma BS 7799-2 de British Estándar, otro organismo de normalización. Esta norma es la principal de la serie, y según ella la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en el tratamiento de la información. Esta norma tiene como finalidad proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de información (SGSI).

El ISO 27001 menciona que el SGSI debe ser dinámico para adaptarse a las nuevas necesidades y objetivos de la organización, así como nuevos requerimientos de seguridad según la naturaleza de los procesos, el tamaño y estructura de la organización.

La norma ISO/ IEC 27001:2005 promueve la adopción de un enfoque del proceso para la gestión de seguridad de la información. Esta norma está alineada con las normas ISO/ IEC 9001:2000 e ISO/ IEC 14001:2004 y se aplica a todos los tipos de organizaciones, grande o pequeña y de cualquier parte del mundo y está diseñada para que el SGSI asegure la selección adecuada y proporcione los controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI).

ISO/ IEC /IEC 27001 es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI.

E. Beneficios esperados en la implantación

Estas actividades anteriores implican tiempo y costos, pero la implantación de la ISO27001 no supone sólo costos, si no, no tendría sentido su aplicación. Son múltiples los beneficios que se derivan de su implementación, lo que hace rentable la misma. Algunos son los siguientes:

- Mayor competitividad que diferencia a la organización.
- Logro de un sistema controlado y metódico que proporciona seguridad.
- Reducción de riesgos.
- Mayor compromiso de mantenimiento y mejora de la seguridad.
- Adaptación a la legislación vigente.
- Realización de auditorías externas, que mejora las actividades de mejora interna.
- Aumento de clientes, ampliación a los que exigen la acreditación en ISO 27001.
- Mayor efectividad en la resolución de incidencias

III. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

III.1. Tipo de Investigación

El tipo de investigación es descriptiva, puesto que se recolecta información a través de las encuestas a los colaboradores de los bancos, datos estadísticos, gráficos y obtener los resultados esperados luego de la implementación así como su análisis.

Se describirá los ángulos o dimensiones de los fenómenos, situaciones y eventos para detallar como son y cómo se manifiestan. Esta investigación por ser de tipo descriptiva buscará especificar o mostrar con precisión los estudios o procesos que son sometidos a análisis, midiendo, evaluando y recolectando datos en relación a las variables de un grupo o población, así como también, por ser de

carácter descriptivo, se pueden hacer predicciones de los resultados aunque sean incipientes (Hernández, 2006).

III.2. Diseño de Investigación

Dentro de la clasificación del tipo de diseño de investigación No Experimental, la presente investigación es Longitudinal, debido a que la investigación se realizó de manera sistemática y no se va a tomar un control sobre la variable independiente, que es un sistema de gestión de seguridad de la información puesto que se va a analizar los cambios a través del tiempo y las decisiones tomadas por la gerencia en cuanto a la aprobación de la implementación para posteriormente ver sus efectos sobre los riesgos de seguridad de información que es la variable dependiente (Hernández, 2006)

III.3. Método de Investigación

El método de investigación es cuantitativo, pues se medirá los fenómenos o eventos ocurridos en la investigación, utilizando datos, encuestas, entrevistas, información y otras herramientas para conocer el resultado final mediante técnicas estadísticas (cuadros, gráficos estadísticos, etc.) (Bernal, 2010) (Hueso, 2012)

III.4. Población

La población lo conforma el personal de las 6 sedes de la entidad bancaria que se encuentran laborado actualmente e involucrados con los procesos seleccionados, es decir, un total de 2761 colaboradores

III.5. Muestra

Viene a ser la cantidad de colaboradores que se deben entrevistar o encuestar para tener una información adecuada con un error estándar menor de 0.015 al 90% de confiabilidad.

$$N = 2761$$

$$\varepsilon = 0.015$$

$$\sigma^2 = (\varepsilon^2) = (0.015)^2 = 0.000225$$

$$s^2 = p(p-1) = 0.9(1-0.9) = 0.09$$

Entonces: $n' = \frac{s^2}{\sigma^2} = \frac{0.09}{0.000225} = 400$

Por lo tanto: $n = \frac{n'}{1+{}^{n'}/_{N}} = \frac{400}{1+{}^{400}/_{2791}} = 350.85$

En conclusión, la muestra es de 351 trabajadores

III.6. Técnicas de recolección de datos e instrumentos

Durante la investigación se aplicaron diversas técnicas que permitieron recopilar la información necesaria para realizar el análisis y la implementación con la finalidad de dar respuesta a los objetivos propuestos. Estas técnicas e instrumentos fueron por medio de diferentes fuentes como son informes, documentos oficiales, encuestas, entrevistas, reportes de asociaciones, datos, testimonios de expertos, revistas y páginas en Internet que incluyen fuentes de listas estadísticas:

- Encuestas: Se utilizó para conocer si los colaboradores cuentan con conocimientos sobre seguridad de información o reciben capacitaciones sobre riesgos en la seguridad de la información en las organizaciones.
- Los instrumentos a utilizarse fueron cuestionarios y pruebas de conocimiento en cuanto a seguridad de la información en la sede de la entidad bancaria.
- Entrevistas: Se entrevistaron a diferentes colaboradores de las áreas en los procesos del SGSI, incluyendo jefaturas con la finalidad de tener información técnica necesaria. El instrumento a utilizarse fue una guía de entrevista que permitió diseñar e implementar el sistema de gestión de seguridad de información en la organización donde laboran.
- Revisión documental: Se utilizó, principalmente, para extraer la información necesaria de las seis sedes de la entidad bancaria para analizar y observar el nivel de implementación de seguridad con la que cuentan y así proponer un sistema de seguridad. Como instrumento que utilizamos fueron la documentación de seguridad de las áreas y guías de información de seguridad.

IV. RESULTADOS

En base a la información recopilada por las entrevistas y encuestas a los 351 colaboradores seleccionados y detallados en la tabla V.1, fue de gran apoyo en la realización de la propuesta de SGSI en las seis sedes principales de la entidad bancaria, teniendo como resultados sobre el nivel de riesgo existente lo mostrado en la tabla V.2.

Tabla V.1
Cantidad de usuarios encuestados

Cantidad de usuarios encuestados	
Usuarios de línea bancaria	224
Sistemas y soporte	23
Helpdesk	49
Seguridad y Accesos	18
Operaciones TI	37

Fuente: Elaboración propia

Tabla V.2
Resultados de la encuesta

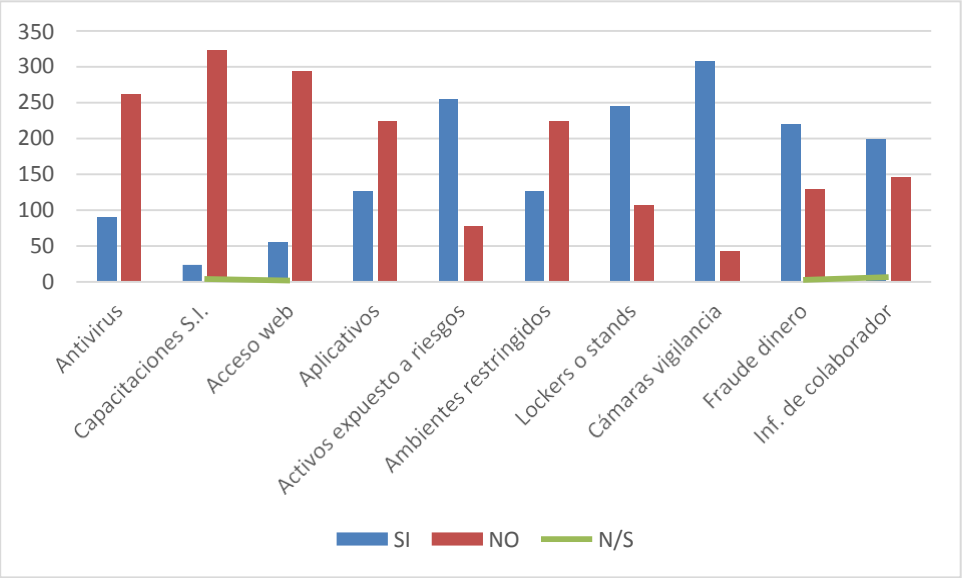
Tecnología de la Información	SI	NO	N/S	Nivel de Riesgo
1. ¿Conoce qué antivirus tiene instalado en su ordenador?	90	261		**Medio**
2. ¿Le brindan capacitaciones sobre Ciberseguridad o seguridad de información?	24	323	4	**Alto**
3. ¿cuenta con acceso a todas las páginas web que usted necesita acceder?	55	294	2	**Alto**
4. ¿Cuenta con todos los aplicativos que usted necesita acceder?	127	224		**Medio**
Ambientes	**SI**	**NO**	**N/S**	**Nivel de Riesgo**
5. ¿Ha observado si usuarios o colaboradores de su área u otras áreas tienen su información expuesta en sus posiciones frente a todos los trabajadores de la empresa? (contraseñas, carteras de clientes, directorios, etc.).	255	77	19	**Alto**
6. ¿Ha ingresado a ambientes físicos restringidos de su empresa?	127	224		**Bajo**
7. (Responder en caso la pregunta 6 es afirmativa), ¿Ingresó con una autorización por su jefe inmediato?	19	108		**Alto**
8. ¿Su empresa le ofrece lockers o stands para guardar su información (libros, folders, documentos de clientes)?	244	107		**Bajo**
9. Los ambientes de operaciones, créditos, tecnología, ¿Cuentan con cámaras de vigilancia para asegurar que los activos no sean manipulados?	308	43		**Medio**
Empresa	**SI**	**NO**	**N/S**	**Nivel de Riesgo**
10. ¿Supo de algún fraude de dinero en su empresa por parte de un cliente o un colaborador?	219	129	3	**Alto**

11. En la empresa donde labora, ¿se debe brindar información de un colaborador si el cliente lo solicita? (nombre, área, jefatura)	199	145	7	**Alto**
12. Con usted mismo u otro colaborador, ¿Presenció algún robo dentro de la empresa?	92	251	8	**Alto**
13. Responder en caso la pregunta 10 es afirmativa ¿informó su jefe inmediato?	16	76		**Medio**
Seguridad del ordenador	**SI**	**NO**	**N/S**	**Nivel de Riesgo**
14. ¿Se realiza un mantenimiento informático periódico sobre el ordenador donde trabaja?	70	273	8	**Medio**
15. (Responder en caso la pregunta 14 es afirmativa), ¿Estuvo presente durante el mantenimiento informático observando que el encargado del trabajo no copie ni elimine su información?	9	61		**Alto**
16. Si trabaja con ordenador portátil, ¿cuenta con un cable de seguridad o anclaje?	69	11		**Medio**
17. Si trabaja con ordenador portátil, ¿cuenta con acceso wifi?	63	17		**Medio**
18. (Responder en caso la pregunta 17 es afirmativa), ¿conoce si el acceso a wifi tiene medida de seguridad para proteger dicha conexión?	2	61		**Alto**
Información personal	**SI**	**NO**	**N/S**	**Nivel de Riesgo**
19. ¿Tiene un respaldo o backup de su información en caso ocurra un desastre natural, robo o eliminación de información?	129	222		**Alto**
20. ¿Está autorizado por su jefatura en descargar archivos o información de su trabajo en su ordenador y copiarlo a un disco externo como un usb?	66	285		**Bajo**
21. (Responder en caso la pregunta 20 es negativa), ¿Descargó o copió archivos a su disco externo por adquirir tal información?	253	32		**Alto**
22. El almacenamiento de sus correos, datos, información, ¿se conecta a través de una ruta compartida hacia otro ordenador?	219	132		**Alto**
23. Colaborador de la empresa o proveedor, ¿conoce la contraseña de su computadora o usuario?	147	204		**Alto**
24. ¿Le ha ocurrido un robo de sus activos en su sitio de trabajo? (Celular, documentos, llaves, dinero, etc.	92	259		**Alto**
Seguridad general	**SI**	**NO**	**N/S**	**Nivel de Riesgo**
25. La empresa donde labora, ¿cuenta con las normas y equipamiento de seguridad de defensa civil?	321	15	15	**Bajo**
26 ¿Cuenta con capacitación periódica sobre medidas de seguridad ante un desastre natural?	260	91		**Medio**
27. Personal de seguridad, ¿Realiza simulacros de evacuación ante un desastre natural?	94	257		**Medio**

Fuente: Elaboración propia

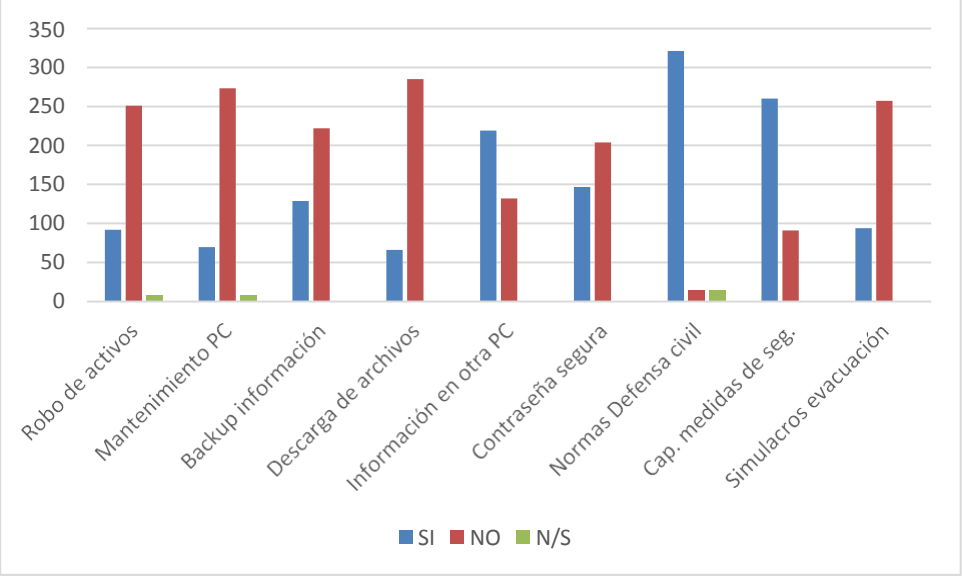
Los siguientes gráficos muestran también el resultado de las encuestas, además, la propuesta de implementar un Sistema de Gestión de Seguridad de la Información se apoya en la norma ISO 27001:2005 e ISO 27001:2013, para las 6 sedes de la entidad bancaria se desarrolló la propuesta en la versión 2005 teniendo como base el modelo Deming (Plan - Do - Check - Act).

Gráfico V.3
Resultados de la encuesta



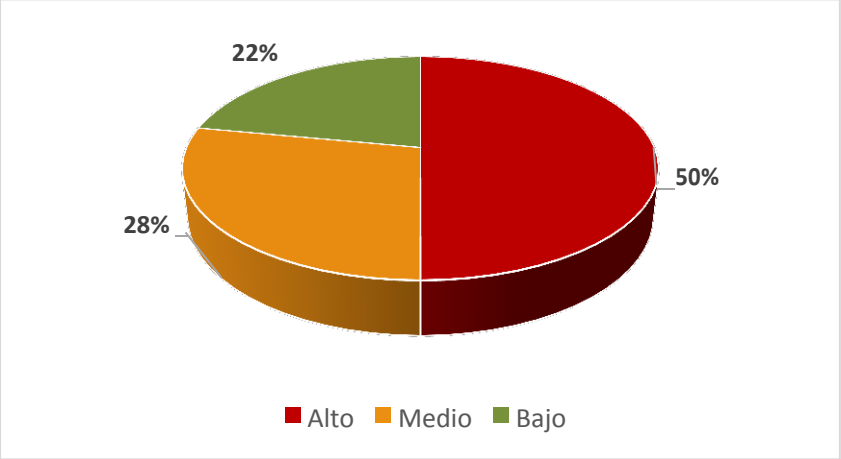
Fuente: Elaboración propia

Gráfico V.4
Resultados de la encuesta



Fuente: Elaboración propia

Gráfico V.5
Nivel del riesgo de los activos en la encuesta



Fuente: Elaboración propia

De los hallazgos obtenidos en cuanto a los niveles de riesgos como resultados de las encuestas, se realiza el diseño de un Sistema de Gestión de Seguridad de la Información en apoyo de la norma ISO27001:2005 estructurando este diseño en base al modelo Deming en sus 4 cláusulas (*Plan*, *Do*, *Check*, *Act*).

IV.1. Planear (*PLAN*)

Primer punto del modelo Deming, donde se establecieron los objetivos de control, procesos, procedimientos y políticas de seguridad del SGSI que fueron relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados de acuerdo con los objetivos generales que cuenta la organización, por tanto se determinaron la definición de la política y el alcance del SGSI.

A. La Organización

Las sedes de la entidad bancaria cuenta con valiosa información, tanto de clientes, empresas, infraestructura, software, etc., el cual basa la administración de seguridad de los activos de información en las políticas generales contenidas en el directorio de políticas que han establecido y del cual no se está auditando.

Con la creación de nuevas políticas de seguridad basadas en el marco de seguridad como lo es el Sistema de Gestión de Seguridad de Información, se busca que todos los participantes (colaboradores y proveedores.) conozcan de este marco normativo de forma individual y en equipo, y así brindar la

seguridad que espera la empresa con sus activos, teniendo en cuenta que se implementará con los niveles adecuados de seguridad.

B. Definición de la política de seguridad

En la presente investigación se presentó la propuesta de definir las políticas de seguridad a la entidad bancaria en sus 6 principales sedes, de los cuales, al llegar a un acuerdo con gerencia de TI solo se seleccionaron las que se presentarán en la propuesta, estas políticas son parte de la herramienta SGSI, detallados a continuación y van acorde con los procesos definidos en el alcance del SGSI.

- Política de Control de acceso
- Política de gestión de activos
- Política para uso de dispositivos móviles
- Política para uso de conexiones remotas
- Política de Responsabilidad por los activos
- Política de áreas seguras
- Política de seguridad en las operaciones
- Política de protección contra software malicioso
- Política de copias de respaldo de la información
- Política de seguridad en las comunicaciones
- Política en el uso de correo electrónico
- Política de uso adecuado de internet
- Política de intercambio de información
- Política de gestión de incidentes de seguridad
- Política del tratamiento y gestión del riesgo en seguridad de la información

C. Alcance del SGSI

En acuerdo con la alta dirección, se tomaron 3 procesos que son considerados como *core* para la organización y así delimitar el SGSI en base a ellos, se muestran en las siguientes figuras:

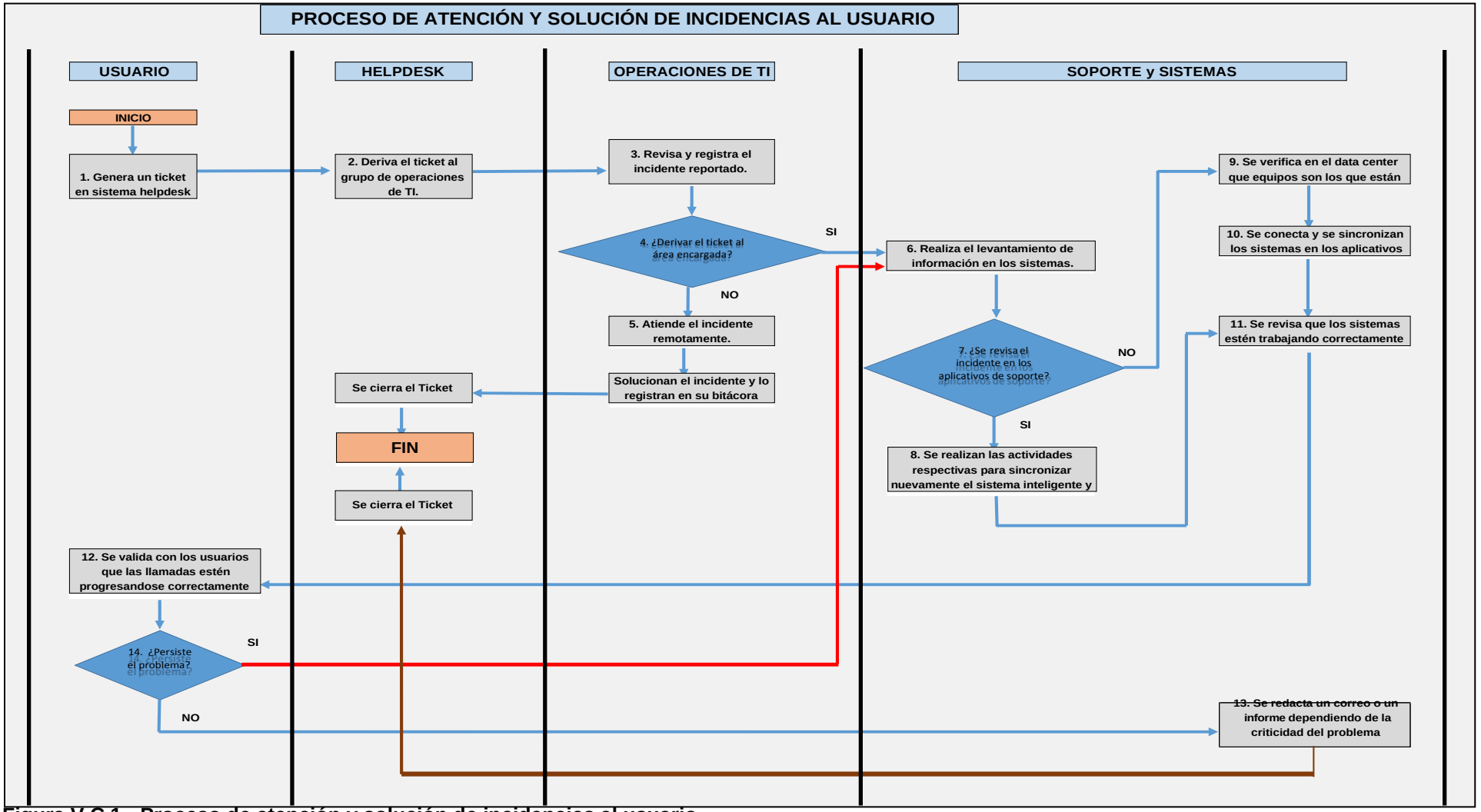


Figura V.C.1 - Proceso de atención y solución de incidencias al usuario
Fuente: Elaboración propia

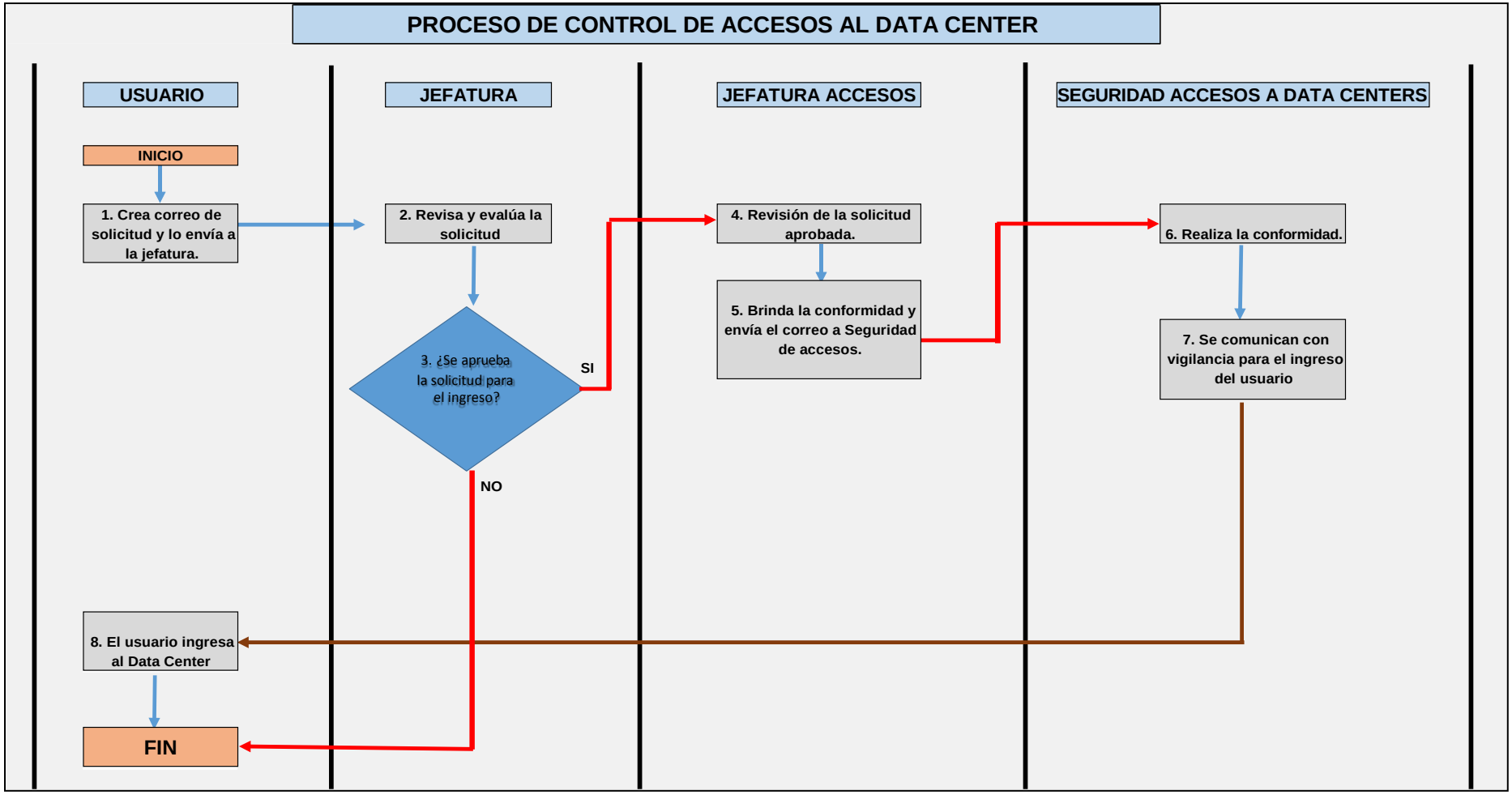


Figura V.C.2 - Proceso de control de accesos al Data Center
Fuente: Elaboración propia

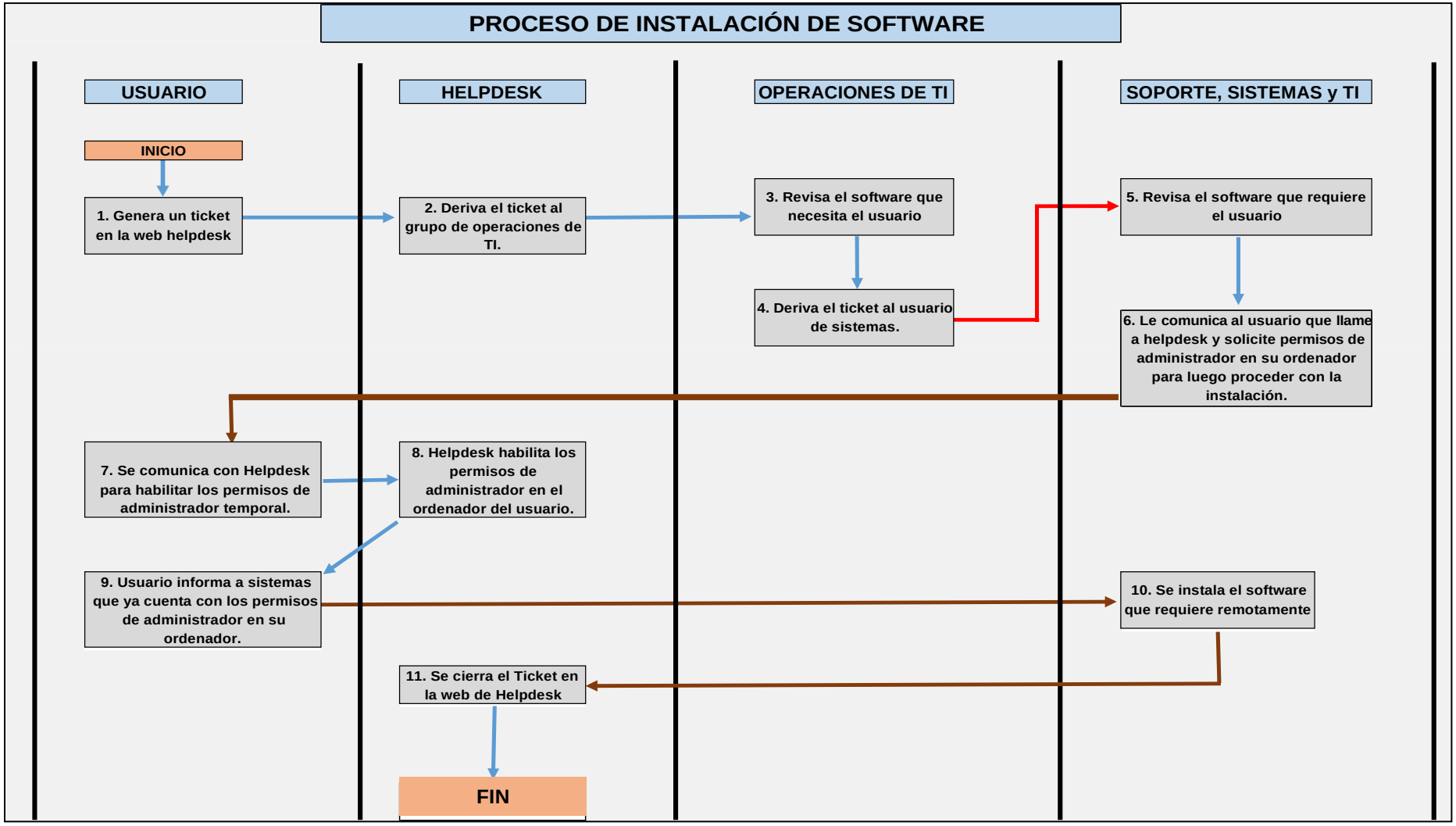


Figura V.C.3 - Proceso de instalación de software
Fuente: Elaboración propia

Cabe indicar que estos procesos solo se propondrán para 6 sedes de una entidad bancaria, que son la sede principal, la sede central, sede de sistemas y sus 3 centros de contacto

D. Revisión por la dirección

El Sistema de gestión de seguridad de información, propuesto para la entidad bancaria, contempla una evaluación periódica, estructurada y auditada el cual está a cargo de la Alta Dirección que permitirá asegurar una adecuada planeación, corrección y cumplimiento de los objetivos, por tanto incluye también la toma de decisiones y acciones necesarias para promover la continuidad del negocio asegurando los activos y los procesos de la organización, alcanzando resultados de eficiencia, eficacia y efectividad.

E. Roles y responsabilidades del SGSI

El SGSI propuesto define roles y funciones de los diferentes participantes, estos roles se alinean y cumplen con las funciones necesarias para poder llevar con éxito la implementación, mantenimiento y monitoreo del SGSI basado en la norma ISO 27001:2005, para ello se debe conocer los responsables de la ejecución, el monitoreo, la auditoría, las áreas auditadas y los terceros que están involucrados dentro del plan de SGSI.

IV.2. Hacer (*DO*)

En este ítem es donde se evalúan los procesos de los riesgos existentes en los activos de las 6 sedes de la entidad bancaria (activos, amenazas, vulnerabilidades) y se prosigue con el diseño para evaluar la política, controles de seguridad y procedimientos para los procesos tomados en el SGSI.

A. Análisis del riesgo

A.1. Identificación de los activos de información

El resultado de las entrevistas y encuestas nos permitió conocer los activos que utiliza el personal que laboran en sus respectivas áreas mostrados en la tabla V.2.1.

Tabla V.2.1
Activos de información del personal por áreas

ACTIVOS DE INFORMACIÓN DEL PERSONAL POR ÁREAS		
Usuario BCP	**Helpdesk**	**Seguridad Accesos**
1. Ordenador	1. Ordenador	1. Ordenador
2. Correo Outlook	2. Correo Outlook	2. Correo Outlook
3. Cartera de clientes	3. Inventario de tickets	3. Registro de ingresos
4. Directorio de usuarios y contraseñas	4. Directorio de usuarios y contraseñas	4. Celulares
5. Internet	5. Internet	5. Internet
6. Chat interno	6. Chat interno	6. Chat interno
7.Teléfonos IP	7. Teléfonos IP	7. Teléfonos IP
8. Información de clientes	8. Aplicativos de Helpdesk	8. Kit de llaves y proxcard
9. Impresoras	9. Impresoras	9. Walkie Talkie
10. Aplicativos de usuario	10. Herramientas de soporte técnico	10. Bitácora de ingresos y trabajos
Jefatura accesos	**Soporte**	**Operaciones de TI**
1. Ordenador	1. Ordenador	1. Ordenador
2. Correo Outlook	2. Correo Outlook	2. Correo Outlook
3. Registro de conformidades	3. Bitácora de incidencias	3. Bitácora de incidencias
4. Directorio de usuarios y contraseñas	4. Inventario de dispositivos	4. Inventario de dispositivos
5. Internet	5. Directorio de usuarios y contraseñas	5. Directorio de usuarios y contraseñas
6. Chat interno	6. Internet	6. Internet
7. Teléfonos IP	7. Chat interno	7. Chat interno
8. Celulares	8. Teléfonos IP	8. Teléfonos IP
9. Impresoras	9. Impresoras	9. Impresoras
10. Aplicativos de accesos	10. Celulares	10. Celulares
11. Kit de llaves y proxcard	11. Aplicativos de Soporte	11. Aplicativos de TI

Fuente: elaboración Propia

A.2. Tasación de los activos identificados

La tasación del activo es el valor del activo frente a la pérdida o falla que afecte la confidencialidad, disponibilidad e integridad, donde se utilizó la escala de Likert (del 1 al 5) como se muestra en la tabla V.2.2.

A.3. Identificación de amenazas y vulnerabilidades

Una vez identificadas las distintas amenazas que pueden afectar un activo se debe evaluar la posibilidad de ocurrencia frente a la vulnerabilidad que puede presentar el activo y evaluado por profesionales de seguridad de información tal como se muestra en la tabla V.2.3.

B. Evaluación del riesgo

B.1. Cálculo del Riesgo

En la tabla V.2.4 se identifican los activos, amenazas y vulnerabilidades, los riesgos se calculan de la combinación de activos que expresan impacto de pérdidas de integridad, confidencialidad y disponibilidad, y del cálculo de la posibilidad de que las amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

B.2. Evaluación del riesgo

Se determina cuáles son aquellas amenazas cuyos riesgos son los más significativos y los primeros que deben analizarse y evaluarse por la gerencia y los profesionales en seguridad de información. Para calificar la prioridad del riesgo se utilizó un rango de 3 valores, los cuales se describen a continuación y se muestran en la tabla V.2.5**.**

Es poco importante prestarle mucho énfasis o esfuerzo al tratamiento del riesgo ya que el activo afectado no es indispensable para la continuidad del negocio.

Se le debe dar importancia moderada al tratamiento del riesgo ya que el activo es importante pero no indispensable para la continuidad y éxito del negocio.

La prioridad que se le debe dar al tratamiento del riesgo es muy importante ya que el activo es indispensable para la continuidad y éxito del negocio.

B.3. Plan de tratamiento de riesgos

Una vez efectuado el análisis y evaluación del riesgo, se debe decidir qué acciones tomar, los riesgos se pueden manejar con una serie de controles para la detección y prevención, como también aceptar el riesgo y transferirlo a otra organización para minimizarlo.

Este plan de tratamiento de riesgos, como se muestra en la tabla V.2.6 contempla también los entregables, es decir, los informes en .pdf que se entregarán a la Alta Gerencia cuando se haya hecho el estudio, análisis o implementación del sistema de gestión de seguridad de la información en las seis sedes de la entidad bancaria.

Tabla V.2.2
Tasación de los activos de información

TASACIÓN DE LOS ACTIVOS DE INFORMACIÓN										
Nº	Activo de Información	Tasación								Total
		Julio Valencia				Michael Salinas				
		C	I	D	Promedio	C	I	D	Promedio	
1	Aplicativos de accesos	5	5	5	5	5	5	5	5	5
2	Aplicativos de Helpdesk	5	5	5	5	5	5	5	5	5
3	Aplicativos del soporte de sistemas	5	5	5	5	5	5	5	5	5
4	Aplicativos del usuario de TI	5	5	5	5	5	5	5	5	5
5	Aplicativos del usuario del banco	3	5	5	4.33	2	5	5	4	4.17
6	Bitácora de incidencias del soporte	4	5	4	4.33	5	5	4	4.67	4.5
7	Bitácora de incidencias del personal TI	4	3	4	3.67	4	4	4	4	3.83
8	Bitácora de ingresos y trabajos	3	4	5	4	2	5	4	3.67	3.83
9	Cartera de clientes	3	4	3	3.33	3	4	4	3.67	3.5
10	Celulares (Helpdesk, TI, Soporte)	5	5	4	4.67	5	5	3	4.33	4.5
11	Celulares (Seguridad y Accesos)	5	4	5	4.67	5	4	5	4.67	4.67
12	Celulares (Usuario del banco)	3	2	3	2.67	2	3	3	2.67	2.67
13	Chat interno (Helpdesk, TI, Soporte)	4	5	5	4.67	5	5	5	5	4.83
14	Chat interno (Seguridad y Accesos)	4	5	5	4.67	5	4	5	4.67	4.67
15	Chat interno (Usuario del banco)	2	2	5	3	3	2	5	3.33	3.17
16	Correo electrónico (Helpdesk, TI, Soporte)	4	5	5	4.67	4	5	5	4.67	4.67
17	Correo electrónico (Seguridad y Accesos)	4	4	5	4.33	4	5	5	4.67	4.5
18	Correo electrónico (Usuario del banco)	3	3	5	3.67	3	3	5	3.67	3.67
19	Directorio de usuarios y contraseñas (Helpdesk)	5	5	5	5	5	5	5	5	5
20	Directorio de usuarios y contraseñas (Soporte)	5	5	4	4.67	5	5	4	4.67	4.67
21	Directorio de usuarios y contraseñas (Personal TI)	5	5	4	4.67	5	5	4	4.67	4.67
22	Herramientas de soporte técnico	4	2	5	3.67	4	1	4	3	3.33
23	Información de clientes	3	4	4	3.67	3	3	3	3	3.33

24	Impresoras	5	4	5	4.67	5	4	5	4.67	4.67
25	Internet	5	4	5	4.67	5	4	5	4.67	4.67
26	Inventario dispositivos de red del soporte	5	5	4	4.67	5	5	5	5	4.83
27	Inventario dispositivos de red personal TI	5	3	4	4	4	4	4	4	4
28	Inventario de tickets	5	4	5	4.67	4	4	5	4.33	4.5
29	Kit de llaves y proxcard	5	3	3	3.67	5	2	3	3.33	3.5
30	Ordenador (Helpdesk, TI, Soporte)	5	5	5	5	5	5	5	5	5
31	Ordenador (Seguridad y Accesos)	4	5	5	4.67	4	4	5	4.33	4.5
32	Ordenador (Usuario del banco)	1	2	4	2.33	1	1	5	2.33	2.33
33	Registros de conformidades	4	4	5	4.33	5	4	5	4.67	4.5
34	Registro de ingresos	5	4	5	4.67	4	4	5	4.33	4.5
35	Teléfonos IP	5	4	5	4.67	5	4	5	4.67	4.67
36	Walkie Talkie	2	3	5	3.33	1	4	4	3	3.17

Fuente: elaboración Propia

Tabla V.2.3
Amenazas y vulnerabilidades por activo de información

AMENAZAS Y VULNERABILIDADES POR ACTIVO DE INFORMACIÓN			
N°	**Activos de información**	**Amenaza**	**Vulnerabilidad**
1	Aplicativos de colaboradores del banco (Accesos, helpdesk, soporte, TI, etc.)	Abuso de privilegios	Cuentas de usuario con rol administrador permanente
		Accesos no permitidos	Contraseñas de seguridad débiles
		Divulgación de información	Mal uso del aplicativo
2	Bitácora de incidencias (Soporte, personal TI)	Alteración de Información	Falta de seguridad en la integridad y confidencialidad de la información de las incidencias.
		Fuga de información de incidencias	
3	Bitácora de ingresos y trabajos a zonas restringidas	Alteración de Información	Carece de seguridad en la integridad y confidencialidad de la información sobre los ingresos y trabajos a las zonas restringidas
		Fuga de información de incidencias	
4	Cartera de clientes	Alteración de Información	Falta de seguridad en la integridad y confidencialidad de la información de la cartera de clientes
		Fuga de información	Contactos de clientes con acceso disponible
5	Celulares	Robo de información	Usuarios no entrenados en temas de seguridad
		Robo del equipo	Carece de control de seguridad en la manipulación del equipo
6	Chat interno (Accesos, Helpdesk, soporte, TI, etc.)	Fuga de información	Cierre de sesión de chat
7	Correo electrónico (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco))	Pérdida de información	No se bloquea el ordenador en ausencia del usuario
		Accesos no permitidos	Manipulación del ordenador en ausencia del usuario
		Utilización por parte de personas no autorizadas para enviar correos a otros usuarios	Intercepción no autorizada de correos electrónicos

8	Directorio de usuarios y contraseñas (Helpdesk, Soporte de sistemas y TI).	Alteración de Información	Seguridad en el uso del directorio de usuarios
		Robo de Contraseñas	Contraseñas expuestas
9	Equipos de red de las plataformas (Soporte)	Alteración de Información	Intercepción no autorizada de correos electrónicos
		Saturación de los discos	Falta de espacio en los discos duros
		Virus	Antivirus no actualizado o sin licencia
		Riesgos de accesos no autorizados desde internet y redes externas hacia los sistemas del Banco	Políticas de seguridad débiles
		Alteración en la conexión de los puertos	Pérdida de conectividad en la red
		Desconexión de los cables eléctricos	Manipulación no autorizada
10	Herramientas de soporte técnico	Robo de material por personal que ingresa temporalmente	Capacitación al personal en seguridad de los equipos y herramientas de trabajo
11	Información de clientes	Alteración de Información	Manipulación de la información por personal no autorizado
		Robo de información	Información expuesta
12	Impresoras (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	Robo de material de impresión	Material de impresión expuesto
		Desconexión del cable eléctrico	Manipulación del cable eléctrico
		Desconfiguración de la impresora	Mal manejo de las funciones de la impresora
13	Internet	Fuga de información	Controles en los protocolos de seguridad de internet
		Virus	Antivirus no actualizado o sin licencia
14	Inventario dispositivos de red (Soporte, TI)	Alteración de Información	Falta de seguridad en el inventario de los dispositivos
		Fuga de información	Carece de un backup
15	Inventario de tickets (Helpdesk)	Alteración de Información	Manipulación de la información por personal no autorizado

		Fuga de información	Carece de un backup del inventario de los tickets
16	Kit de llaves y proxcard	Robo del kit de llaves y proxcard	Falta de seguridad en el kit de herramientas
		Acceso no permitidos	Carece de controles de seguridad en el uso de las llaves a los ambientes y la proxcard
17	Ordenador (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	Alteración de Información	Ausencia de seguridad en los archivos que contiene información sensible
		Robo de Contraseñas	Capacitación al personal sobre seguridad
		Virus	Antivirus no actualizado o sin licencia
		Desconexión de su cable eléctrico	Manipulación no autorizada de personal
		Robo de los equipos del ordenador	Carece de cámaras de vigilancia en los ambientes de trabajo
18	Registros de conformidades	Alteración de Información	Carece de registro extra de conformidades
19	Registro de ingresos	Alteración de Información	Capacitación sobre el registro de ingresos a zonas restringidas
		Accesos no solicitados	Mala gestión de roles y responsabilidades
20	Teléfonos IP	Robo del dispositivo	Cámaras de vigilancia en los ambientes de trabajo
21	Walkie Talkie	Robo del dispositivo	Dependencia exclusiva de un solo personal

Fuente: elaboración Propia

Tabla V.2.4
Cálculo del riesgo por activo de información

CÁLCULO SOBRE LA POSIBILIDAD DE OCURRENCIA DE VULNERABILIDAD Y AMENAZAS						
N°	**Activos de información**	**Amenaza**	**Posibilidad de ocurrencia de la Amenaza**	**Posibilidad de ocurrencia de la Vulnerabilidad**	**Impacto**	**Riesgo**
1	Aplicativos de accesos	Abuso de privilegios	1	2	3	3
		Accesos no permitidos	2	3	2	4
2	Aplicativos de Helpdesk	Abuso de privilegios	1	1	4	4
		Accesos no permitidos	2	2	5	10
		Mal manejo del aplicativo	1	1	4	4
3	Aplicativos del Soporte de sistemas	Abuso de privilegios	1	2	2	2
		Accesos no permitidos	1	2	5	5
		Mal manejo del aplicativo	2	1	5	10
4	Aplicativos del usuario de TI	Abuso de privilegios	2	1	4	8
		Mal manejo del aplicativo	1	1	4	4
		Accesos no permitidos	1	2	3	3
5	Aplicativos del usuario del banco	Abuso de privilegios	3	1	2	6
		Accesos no permitidos	4	4	4	16
		Mal manejo del aplicativo	5	5	5	25
6	Bitácora de incidencias del soporte	Alteración de Información	2	1	4	8
		Fuga de información de incidencias	1	2	3	3
7	Bitácora de incidencias del personal TI	Alteración de Información	2	1	4	8
		Fuga de información de incidencias	3	2	3	9
8	Bitácora de ingresos y trabajos a zonas restringidas	Alteración de Información	3	2	2	6
		Fuga de información de incidencias	4	3	2	8
9	Cartera de clientes	Alteración de Información	5	4	5	25
		Fuga de información	5	5	5	25
10	Celulares	Robo de información	2	2	3	6

		Robo del equipo	1	2	1	1
11	Chat interno (Helpdesk, TI, Soporte)	Fuga de información	1	1	3	3
12	Chat interno (Seguridad y Accesos)	Fuga de información	2	2	2	4
13	Chat interno (Usuario del banco)	Fuga de información	5	5	5	25
14	Correo electrónico (Helpdesk, TI, Soporte)	Accesos no permitidos	1	1	2	2
		Pérdida de información	2	2	3	6
		Utilización por parte de personas no autorizadas para enviar correos a otros usuarios	1	1	3	3
15	Correo electrónico (Seguridad y Accesos)	Accesos no permitidos	2	2	2	4
		Pérdida de información	1	3	3	3
		Utilización por parte de personas no autorizadas para enviar correos a otros usuarios	2	2	3	6
16	Correo electrónico (Usuario del banco)	Accesos no permitidos	5	4	3	15
		Pérdida de información	4	4	5	20
		Utilización por parte de personas no autorizadas para enviar correos a otros usuarios	5	5	5	25
17	Directorio de usuarios y contraseñas (Helpdesk)	Alteración de Información	2	2	1	2
		Robo de Contraseñas	1	2	3	3
18	Directorio de usuarios y contraseñas (Soporte)	Alteración de Información	1	1	2	2
		Robo de Contraseñas	2	2	2	4
19	Directorio de usuarios y contraseñas (Personal TI)	Alteración de Información	1	1	3	3
		Robo de Contraseñas	1	1	3	3
20	Equipos de red de las plataformas (Soporte)	Alteración de Información	4	2	4	16
		Saturación de los discos	5	3	5	25
		Virus	1	2	5	5

		Riesgos de accesos no autorizados desde internet y redes externas hacia los sistemas del Banco	5	3	5	25
		Alteración en la conexión de los puertos	5	3	5	25
		Desconexión de los cables eléctricos	5	4	5	25
21	Herramientas de soporte técnico	Robo de material por personal que ingresa temporalmente	4	2	2	8
22	Información de clientes	Alteración de Información	5	4	4	20
		Robo de información	5	3	4	20
23	Impresoras (Helpdesk, TI, Soporte)	Robo de material de impresión	2	2	1	2
		Desconexión del cable eléctrico	1	1	2	2
		Desconfiguración de la impresora	1	1	2	2
24	Impresoras (Usuarios del banco)	Robo de material de impresión	4	4	3	12
		Desconexión del cable eléctrico	5	3	3	15
		Desconfiguración de la impresora	5	4	4	20
25	Internet	Fuga de información	4	3	3	12
		Virus	1	2	4	4
26	Inventario dispositivos de red del soporte	Alteración de Información	2	2	2	4
27	Inventario dispositivos de red personal TI	Alteración de Información	1	1	2	2
28	Inventario de tickets (Helpdesk)	Fuga de información	1	2	1	1
29	Kit de llaves y proxcard	Robo del kit de llaves y proxcard	2	1	1	2
		acceso no permitidos	3	3	2	6
30	Ordenador (Helpdesk, TI, Soporte)	Alteración de Información	2	2	2	4
		Robo de Contraseñas	1	1	4	4
		Virus	1	1	3	3
		Desconexión de su cable eléctrico	2	1	2	4
		Robo de los equipos del ordenador	3	2	3	9

31	Ordenador (Seguridad y Accesos)	Alteración de Información	2	2	2	4
		Robo de Contraseñas	2	2	1	2
		Virus	1	1	2	2
		Desconexión de su cable eléctrico	3	2	3	9
		Robo de los equipos del ordenador	4	3	3	12
32	Ordenador (Usuario del banco)	Alteración de Información	5	4	4	20
		Robo de Contraseñas	5	5	5	25
		Virus	2	2	2	4
		Desconexión de su cable eléctrico	5	4	2	10
		Robo de los equipos del ordenador	4	4	2	8
33	Registros de conformidades	Alteración de Información	2	2	1	2
34	Registro de ingresos	Alteración de Información	3	1	2	6
		Accesos no solicitados	3	3	1	3
35	Teléfonos IP	Robo del dispositivo	1	1	1	1
36	Walkie Talkie	Robo del dispositivo	2	2	1	2

Fuente: elaboración Propia

Tabla V.2.5
Evaluación del riesgo por activo de información

EVALUACIÓN DEL RIESGO										
Riesgos			Criterios para evaluar la importancia							Estrategias del tratamiento del Riesgo
N°	Activos de información	Amenaza	Deterioro de Imagen de la Empresa	Tiempo de Recuperación	Impacto Económico	Impacto en la Organización (Personal)	Impacto en las Operaciones	Total	Nivel del Riesgo	
1	Aplicativos de colaboradores del banco (Accesos, Helpdesk, soporte, TI, etc.)	Abuso de privilegios	2	1	2	3	4	12	MEDIO	Mitigar
		Accesos no permitidos	1	2	3	4	3	13	MEDIO	Mitigar
		Divulgación de información	3	3	4	2	2	14	MEDIO	Mitigar
2	Bitácora de incidencias (Soporte, personal TI)	Alteración de Información	2	2	2	3	4	13	MEDIO	Mitigar
		Fuga de información de incidencias	2	2	3	2	5	14	MEDIO	Mitigar
3	Bitácora de ingresos y trabajos a zonas restringidas	Alteración de Información	3	2	1	2	3	11	MEDIO	Mitigar
		Fuga de información de incidencias	2	3	2	2	4	13	MEDIO	Mitigar
4	Cartera de clientes	Alteración de Información	4	2	3	4	5	18	ALTO	Mitigar
		Fuga de información	5	4	4	5	5	23	ALTO	Mitigar
5	Celulares	Robo de información	3	2	4	4	4	17	ALTO	Mitigar
		Robo del equipo	4	1	3	3	3	14	MEDIO	Mitigar
6	Chat interno (Accesos, Helpdesk, soporte, TI, etc.)	Fuga de información	4	2	4	4	4	18	ALTO	Mitigar
7	Correo electrónico	Pérdida de	5	4	4	4	5	22	ALTO	Mitigar

	(Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco))	información								
		Accesos no permitidos	4	3	3	3	4	17	ALTO	Mitigar
		Utilización por parte de personas no autorizadas para enviar correos a otros usuarios	5	2	4	4	5	20	ALTO	Mitigar
8	Directorio de usuarios y contraseñas (Helpdesk, Soporte de sistemas y TI).	Alteración de Información	3	2	2	3	3	13	MEDIO	Mitigar
		Robo de Contraseñas	2	1	2	4	4	13	MEDIO	Mitigar
9	Equipos de red de las plataformas (Soporte)	Alteración de Información	2	4	2	4	4	16	ALTO	Mitigar
		Saturación de los discos	1	5	5	3	5	19	ALTO	Transferir
		Virus	3	4	5	2	5	19	ALTO	Transferir
		Riesgos de accesos no autorizados desde internet y redes externas hacia los sistemas del Banco	4	5	4	4	5	22	ALTO	Transferir
		Alteración en la conexión de los puertos	2	4	4	2	5	17	ALTO	Mitigar
		Desconexión de los cables eléctricos	1	2	3	2	5	13	MEDIO	Transferir
10	Herramientas de soporte técnico	Robo de material por personal que ingresa temporalmente	1	2	3	2	4	12	MEDIO	Transferir
11	Información de clientes	Alteración de Información	4	3	2	4	4	17	ALTO	Mitigar

		Robo de información	5	4	3	5	5	22	ALTO	Mitigar
12	Impresoras (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	Robo de material de impresión	2	1	3	2	4	12	MEDIO	Transferir
		Desconexión del cable eléctrico	1	2	2	1	4	10	BAJO	Evitar
		Desconfiguración de la impresora	2	1	2	2	4	11	MEDIO	Evitar
13	Internet	Fuga de información	4	2	3	2	4	15	MEDIO	Mitigar
		Virus	3	4	4	2	5	18	ALTO	Transferir
14	Inventario dispositivos de red (Soporte, TI)	Alteración de Información	2	2	2	1	4	11	MEDIO	Mitigar
		Fuga de información	1	2	3	2	5	13	MEDIO	Mitigar
15	Inventario de tickets (Helpdesk)	Alteración de Información	1	1	2	1	4	9	BAJO	Evitar
		Fuga de información	2	2	2	2	3	11	MEDIO	Mitigar
16	Kit de llaves y proxcard	Robo del kit de llaves y proxcard	1	2	3	2	4	12	MEDIO	Transferir
		Acceso no permitidos	3	3	2	3	3	14	MEDIO	Transferir
17	Ordenador (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	Alteración de Información	2	2	1	3	4	12	MEDIO	Mitigar
		Robo de Contraseñas	2	2	2	4	3	13	MEDIO	Mitigar
		Virus	1	4	4	2	5	16	ALTO	Transferir
		Desconexión de su cable eléctrico	1	1	4	2	4	12	MEDIO	Transferir
		Robo de los equipos del ordenador	4	3	4	4	5	20	ALTO	Transferir
18	Registros de conformidades	Alteración de Información	3	3	2	2	3	13	MEDIO	Mitigar
19	Registro de ingresos	Alteración de Información	2	2	2	1	3	10	BAJO	Evitar

		Accesos no solicitados	3	3	1	2	4	13	MEDIO	Transferir
20	Teléfonos IP	Robo del dispositivo	4	1	5	4	4	18	ALTO	Transferir
21	Walkie Talkie	Robo del dispositivo	4	3	4	5	3	19	ALTO	Transferir

Fuente: elaboración Propia

Tabla V.2.6
Plan de tratamiento del riesgo

PLAN DE TRATAMIENTO DE RIESGO						
N°	**Activos de información**	**Objetivos de Control**	**Controles**	**Recursos**	**Responsable**	**Plazo de Entrega (días)**
1	Aplicativos de colaboradores del banco	A.12.2 Proceso correcto en aplicaciones	A.12.2.1. Validación de los datos de entrada A.12.2.4 Validación de los datos de salida	Instalador upgrade de los aplicativos	Helpdesk, soporte, TI	7
2	Bitácora de incidencias (Soporte, personal TI)	A.10.7 Utilización y seguridad de los medios de información	A.10.7.3 Procedimientos de manipulación de la información A.10.7.4 Seguridad de la documentación de sistemas	Software de registro a bitácoras con ingreso seguro	Soporte y TI	6
3	Bitácora de ingresos y trabajos a zonas restringidas	A.10.1 Procedimientos y responsabilidades de operación	A.10.1.2 Gestión de cambios A.10.1.1 Documentación de procedimientos operativos	Software para registro de accesos	Seguridad y Accesos	6
4	Cartera de clientes	A.8.1 Previo al empleo	A.8.1.1 Roles y responsabilidades A.8.1.2 Investigación A.8.1.3 Términos y condiciones de la relación laboral	Software de almacenamiento de cartera de clientes, con acceso seguro	Usuarios del banco	8
5	Celulares	A.7.1 Responsabilidad por los activos A.8.3 Finalización o cambio de empleo	A.7.1.1 Inventario de activos A.7.1.2 Uso aceptable de los activos A.8.3.2 Devolución de activos	Capacitación sobre la seguridad y el uso adecuado del equipo	Seguridad y Accesos	4
6	Chat interno (Accesos, helpdesk, soporte, TI, etc.)	A.10.8 Intercambio de información A.11.3 Responsabilidades de los usuarios	A.10.8.1 Políticas y procedimientos para el intercambio de información A.11.3.1 Uso de contraseñas	Chat con opción de cierre de sesión automático	Helpdesk	4

7	Correo electrónico (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco))	A.10.8 Intercambio de información	A.10.8.1 Políticas y procedimientos para el intercambio de información A.10.8.4 Seguridad del correo electrónico	Opción de habilitar contraseña en outlook	Helpdesk	4
8	Directorio de usuarios y contraseñas (Helpdesk, Soporte de sistemas y TI).	A.11.2 Gestión de acceso de usuarios	A.11.2.3 Gestión de contraseñas de usuario	Software de registro de directorio con ingreso seguro	Helpdesk, Soporte de sistemas y TI	5
9	Equipos de red de las plataformas (Soporte)	A.9.2 Seguridad de los equipos A.10.4 Protección contra software malicioso A.11.4 Control de acceso a la red	A.9.2.1 Ubicación y protección de equipos A.9.2.2 Suministro eléctrico A.9.2.3 Seguridad e el cableado A.9.2.4 Mantenimiento de equipos A.9.2.6 Seguridad en el re-uso o eliminación de equipos A.9.2.7 Retiro de propiedad A.10.4.1 Controles contra software malicioso A.11.4.2 Autenticación de usuarios para conexiones externas	Actualizaciones de licencias, software, upgrades y equipos	Soporte y TI	8
10	Herramientas de soporte técnico	A.7.1 Responsabilidad por los activos A.8.3 Finalización o cambio de empleo	A.7.1.1 Inventario de activos A.7.1.2 Uso aceptable de los activos A.8.3.2 Devolución de activos	Herramientas nuevas	Soporte	5
11	Información de clientes	A.8.1 Previo al empleo	A.8.1.1 Roles y responsabilidades A.8.1.2 Investigación A.8.1.3 Términos y condiciones de la relación laboral	Software de registro de información de clientes con acceso seguro	Usuarios del banco	7

12	Impresoras (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	A.7.1 Responsabilidad por los activos	A.7.1.2 Uso aceptable de los activos	Capacitación para el uso adecuado de la impresora	Soporte	4
13	Internet	A.10.4 Protección contra software malicioso A.11.1 Requisitos de negocio para el control de accesos A.11.2 Gestión de acceso de usuarios	A.10.4.1 Controles contra software malicioso A.11.1.1 Política de control de accesos A.11.2.2 Gestión de privilegios	Actualización de antivirus	Helpdesk	4
14	Inventario dispositivos de red (Soporte, TI)	A.10.1 Procedimientos y responsabilidades de operación	A.10.1.2 Gestión de cambios A.10.1.1 Documentación de procedimientos operativos	Software de registro para inventario de equipos con acceso seguro	Soporte y TI	5
15	Inventario de tickets (Helpdesk)	A.7.2 Clasificación de la información	A.7.2.2 Etiquetado y tratamiento de la información	Software de registro para inventario de tickets con acceso seguro	Helpdesk	3
16	Kit de llaves y proxcard	A.7.1 Responsabilidad por los activos A.8.3 Finalización o cambio de empleo	A.7.1.1 Inventario de activos A.7.1.2 Uso aceptable de los activos A.8.3.2 Devolución de activos	Estuche para llaves con candado	Seguridad y Accesos	3
17	Ordenador (Helpdesk, TI, Soporte, Seguridad y accesos, usuarios del banco)	A.7.1 Responsabilidad por los activos A.10.4 Protección contra software malicioso A.11.3 Responsabilidades de los usuarios	A.7.1.2 Uso aceptable de los activos A.10.4.1 Controles contra software malicioso A.11.3.3 Política de pantalla y escritorio limpio	Actualizaciones de licencias, software, upgrades y mantenimiento de ordenadores	Helpdesk, soporte y TI	7

18	Registros de conformidades	A.6.2 Seguridad del acceso a terceras partes	A.6.2.1 Identificación de riesgos por el acceso de terceros A.6.2.3 Requisitos de seguridad en contratos con terceros	Software de registro de conformidades con acceso seguro	Seguridad y Accesos	4
19	Registro de ingresos (Accesos)	A.9.1 Áreas seguras	A.9.1.1 Seguridad física perimetral A.9.1.2 Controles físicos de entradas A.9.1.4 Protección contra amenazas externas y ambientales A.9.1.5 El trabajo en las áreas seguras	Software de registro de accesos a zonas restringidas	Seguridad y Accesos	4
20	Teléfonos IP	A.9.2 Seguridad de los equipos	A.9.2.1 Ubicación y protección de equipos A.9.2.2 Suministro eléctrico A.9.2.3 Seguridad e el cableado A.9.2.4 Mantenimiento de equipos	Actualización de software de teléfonos y compra de nuevos equipos	Soporte y TI	5
21	Walkie Talkie (Seguridad)	A.7.1 Responsabilidad por los activos A.8.3 Finalización o cambio de empleo	A.7.1.1 Inventario de activos A.7.1.2 Uso aceptable de los activos A.8.3.2 Devolución de activos	Capacitación para el uso adecuado del Walkie Talkie	Seguridad y Accesos	4

Fuente: elaboración Propia

B.4. Matriz de Probabilidad e impacto de riesgo

La matriz de probabilidad de ocurrencia e impacto del riesgo muestra la combinación de los dos factores y nace del cuadro de la Evaluación del Riesgo, se utiliza para conocer la prioridad que tiene cada riesgo, Esta prioridad del riesgo se calcula al multiplicar la probabilidad de ocurrencia de la amenaza por el impacto, los riesgos calculados se categorizan como Altos, Medios y Bajos, teniendo en cuenta que los riesgos Altos sombreados de color rojo son los que mayormente ocurren por colaboradores que no cuentan con conocimientos o capacitaciones en seguridad de la información.

La zona roja significa que son riesgos muy probables y de muy alto impacto, la zona Amarilla son riesgos desde situaciones improbables y de impacto medio hasta situaciones muy probables pero de impacto bajo, finalmente los de la zona Verde son riesgos improbables pero de bajo impacto.

Tabla V.2.7
Matriz de Probabilidad e impacto de riesgo

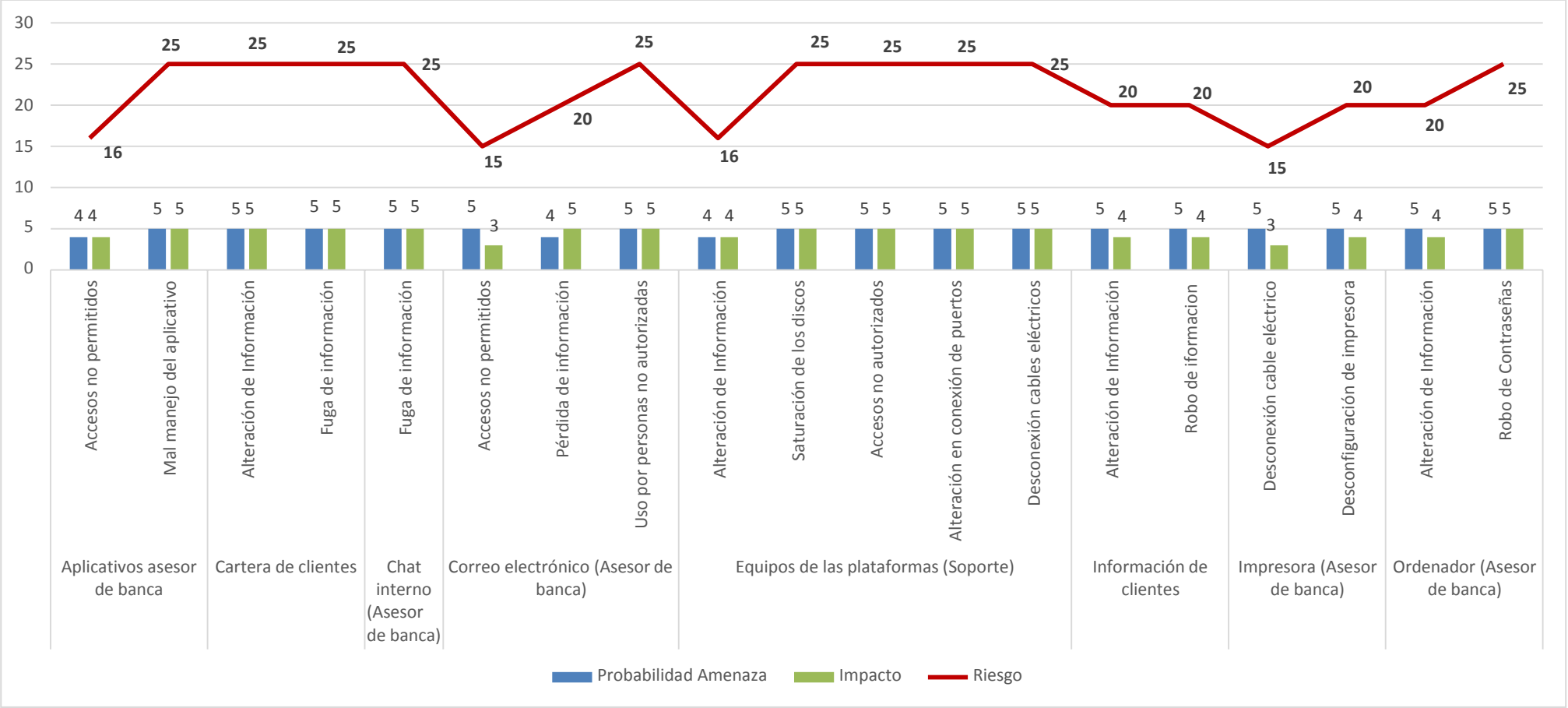
Niveles del Riesgo

Posibilidad de Ocurrencia de Amenaza						
8	10	20	25	25	25	25
8	9	15	20	25	25	25
6	8	12	16	20	25	25
4	6	9	12	16	20	25
3	4	6	9	12	15	20
3	4	4	6	8	10	10
2	3	4	5	6	8	8
2	3	4	4	5	6	6
2	2	3	4	4	4	4
2	2	2	3	4	4	4
1	2	2	2	3	3	3
1	1	2	2	2	3	3

Impacto

Fuente: Elaboración propia

Gráfico V.6
Niveles del riesgo según impacto por probabilidad



Fuente: Elaboración propia

B.5. Costos asociados al proyecto

La siguiente tabla muestra el costo que presenta cada actividad dentro del proyecto del SGSI con la organización, donde se detalla la cantidad de días que toma cada actividad y contrastando con el cronograma de implementación mencionado en la tabla III.3.2. El costo total del proyecto es de 200082 dólares americanos, este monto es evaluado por las Altas Gerencias del banco (administrativas, proyectos, Tecnologías de la Información y operaciones), por tal motivo se espera la conformidad de los responsables para poner en marcha la ejecución del proyecto SGSI a través de empresas especialistas en la implementación de proyectos de seguridad de información.

Tabla V.2.8
Propuesta de proyecto de implementación de SGSI

Propuesta de Proyecto de Implementación del SGSI					
Código del Proyecto	**Descripción del proyecto**	**Tiempo de ejecución (días)**	**Cantidad (Unid.)**	**Costo ($)**	**Total ($)**
PGS_SGSI0034	Chat con opción de cierre de sesión automático (upgrade)	2	1	58	58
PGS_SGSI0037	Opción de habilitar contraseña en outlook (upgrade)	2	1	39	39
PGS_SGSI0016	Actualizaciones de Software a los ordenadores del call center	3	1	300	300
PGS_SGSI0019	Actualizaciones de Software a los equipos de TI, Soporte y Operaciones	3	1	300	300
PGS_SGSI0014	Actualizaciones de Software a los equipos de Seguridad y accesos	3	1	300	300
PGS_SGSI0013	Actualizaciones de Software a los equipos del data center	2	1	410	410
PGS_SGSI0017	Actualizaciones de licencias a los ordenadores del call center	2	224	45	10080
PGS_SGSI0015	Actualizaciones de licencias a los ordenadores de TI, Soporte y Operaciones	2	109	45	4905
PGS_SGSI0010	Actualizaciones de licencias a los ordenadores de Seguridad y accesos	1	18	45	810
PGS_SGSI0012	Actualizaciones de licencias a los equipos del data center	3	58	87	5046
PGS_SGSI0025	Actualizaciones de licencias a las impresoras	2	19	29	551
PGS_SGSI0018	Actualización de antivirus en las computadoras y laptops	3	1	69	69
PGS_SGSI0011	Actualización de antivirus en los servidores	3	1	89	89

PGS_SGSI0022	Actualización de antivirus en los equipos móviles (celulares)	1	127	53	6731
PGS_SGSI0020	Licencias para los equipos de telefonía para el call center	2	224	48	10752
PGS_SGSI0043	Capacitación para el uso adecuado del walkie talkie	1	-	100	100
PGS_SGSI0047	Capacitación para el uso adecuado de la impresora	1	-	100	100
PGS_SGSI0040	Capacitación sobre seguridad de la información	3	-	350	350
PGS_SGSI0041	Capacitación sobre seguridad informática	3	-	400	400
PGS_SGSI0081	Estuche para llaves con candado	4	6	40	240
PGS_SGSI0089	Kit Herramientas nuevas (para el técnico de soporte)	4	6	45	270
PGS_SGSI0051	Mantenimiento de hardware de ordenadores del call center	4	224	15	3360
PGS_SGSI0053	Mantenimiento de hardware de ordenadores de TI, Soporte y Operaciones	3	109	15	1635
PGS_SGSI0057	Mantenimiento de hardware de ordenadores de Seguridad y accesos	2	18	15	270
PGS_SGSI0115	Equipo de control biométrico a zonas restringidas	4	3	1950	5850
PGS_SGSI0116	Renovación equipo de control biométrico a los ambientes de trabajo	7	12	1950	23400
PGS_SGSI0111	Renovación de equipos de telefonía para el call center	6	224	220	49280
PGS_SGSI0119	Renovación cámaras de seguridad en los ambientes de trabajo	8	80	473	37840
PGS_SGSI0070	Software de registro de conformidades con acceso seguro	2	1	79	79
PGS_SGSI0073	Software de registro para inventario de equipos con acceso seguro	2	1	84	84
PGS_SGSI0078	Software de registro para inventario de tickets con acceso seguro	2	1	68	68
PGS_SGSI0072	Software de almacenamiento de cartera e información de clientes, con acceso seguro	2	1	86	86
PGS_SGSI0074	Software de registro a bitácoras con ingreso seguro	2	1	111	111
PGS_SGSI0075	Software de registro de directorio de contactos con ingreso seguro	2	1	119	119
PGS_SGSI0007	Mano de obra (6 especialistas)	96	6	6000	36000

Fuente: elaboración Propia

B.6. Objetivos de control y controles

Del plan de tratamiento de riesgos, la organización aceptó los controles adecuados para trabajar con cada activo de información, el cual tiene como función lo siguiente.

1. **Dominio 6: Organización de la seguridad de la información**

   Gestionar la seguridad de la información dentro de la organización. Se establecerá una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la institución. Se deberá desarrollar contactos con especialistas externos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como tener un punto de enlace para tratar las incidencias de seguridad. Asimismo, se fomentará un enfoque multidisciplinario de la seguridad de la información, que, implique la cooperación y la colaboración de la comunidad usuaria entera

2. **Dominio 7: Gestión de activos**

   Mantener una protección adecuada sobre los activos de la institución. Se deberá adjudicar la responsabilidad de todos los activos de información
   importantes y se deberá asignar un propietario. La responsabilidad sobre los activos ayuda a asegurar que se mantiene la protección adecuada. Se deberá identificar los propietarios para todos los activos importantes, y se asignará la responsabilidad del mantenimiento de los controles apropiados. La responsabilidad de la implantación de controles deberá delegarse. Sin embargo, la responsabilidad se mantendrá en el propietario designado del activo

3. **Dominio 8: Seguridad en recursos humanos**

   Reducir los riesgos de errores humanos, robos, infidencia, fraudes o mal uso de las instalaciones y los servicios. La seguridad se contemplará desde las etapas de selección de personal, incluirse en los contratos y seguirse durante el desarrollo de la relación laboral.

Se deberá filtrar adecuadamente los candidatos, sobre todo para tareas sensibles. Todos los empleados y los terceros, usuarios de aplicaciones de tratamiento de información, deberán firmar una cláusula de confidencialidad (no divulgación)

4. **Dominio 9: Seguridad física y de entorno**

   Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la Institución. Los recursos para el tratamiento de información crítica o sensible para la organización deberán ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se dará protección física contra accesos no autorizados, daños e interferencias

5. **Dominio 10: Gestión de comunicaciones y operaciones**

   Asegurar la operación correcta y segura de los recursos de tratamiento de información. Se deberán establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información.

6. **Dominio 11: Control de accesos**

   Controlar los accesos a la información. Se deberá controlar el acceso a la información y los procesos críticos de la institución sobre la base de los requisitos de seguridad y objetivos institucionales. Se deberá tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

7. **Dominio 12: Adquisición, desarrollo y mantenimiento de sistemas**

   Asegurar que la seguridad esté imbuida dentro de los sistemas de información. Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad deberán ser identificados y

consensuados antes de desarrollar los sistemas de información. Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, deberán ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información

B.7. Declaración de Aplicabilidad

En el documento de declaración de aplicabilidad se detallan los objetivos de control aplicables al SGSI el cual permitirá conocer cuáles se implementarán en la organización.

Tabla V.2.9
Declaración de aplicabilidad del SGSI

DECLARACIÓN DE APLICABILIDAD				
Ítem	**Objetivos de Control**	**Controles**	**Aplicabilidad**	**Comentario sobre el diseño**
1	A.6.2 Seguridad del acceso a terceras partes	A.6.2.1 Identificación de riesgos por el acceso de terceros	Si Aplica	Realizar un cuadro de accesos a los terceros
		A.6.2.3 Requisitos de seguridad en contratos con terceros	Si Aplica	Los contratos con terceros incluyen requerimientos de seguridad para el ingreso a las instalaciones de la compañía
2	A.7.1 Responsabilidad por los activos	A.7.1.1 Inventario de activos	Si Aplica	Se cuenta con un inventario de activos de información en la cual es actualizado en la realización de la propuesta
		A.7.1.2 Uso aceptable de los activos	Si Aplica	En el inventario de los activos de información se encuentran documentados los responsables de dichos activos
3	A.7.2 Clasificación de la información	A.7.2.2 Etiquetado y tratamiento de la información	Si Aplica	El etiquetado y tratamiento de la información se redactaría en las políticas de seguridad de la información
4	A.8.1 Previo al empleo	A.8.1.1 Roles y responsabilidades	Si Aplica	Se tiene identificado los requisitos de seguridad de los puestos de cada colaborador y sus responsabilidades
		A.8.1.2 Investigación	Si Aplica	Se identifican los antecedentes de los candidatos que ocuparán los nuevos cargos, incluyendo terceros
		A.8.1.3 Términos y condiciones de la relación laboral	Si Aplica	Se debe de firmar un Contrato de Confidencialidad que es firmado entre las gerencias y el personal al término de su vínculo laboral

5	A.8.3 Finalización o cambio de empleo	A.8.3.2 Devolución de activos	Si Aplica	Al finalizar el contrato con la compañía, los jefes de cada colaborador que termina su vínculo laboral es responsable de verificar que todos los activos de información sean devueltos
6	A.9.1 Áreas seguras	A.9.1.1 Seguridad física perimetral	Si Aplica	Se instalará controles de acceso electrónico, como tarjetas proxcard, puertas metálicas, etc.
		A.9.1.2 Controles físicos de entradas	Si Aplica	Los controles se detallarían en los documentos de políticas de seguridad de la información
		A.9.1.4 Protección contra amenazas externas y ambientales	Si Aplica	La empresa debe renovar sus implementos de seguridad ambiental, como extintores, detectores de humo, sistema de aire acondicionado.
		A.9.1.5 El trabajo en las áreas seguras	Si Aplica	El detalle se redactaría en las políticas de seguridad de la información
7	A.9.2 Seguridad de los equipos	A.9.2.1 Ubicación y protección de equipos	Si Aplica	Se redactará un documento detallando la ubicación y protección de equipos
		A.9.2.2 Suministro eléctrico	Si Aplica	La compañía contará con mantenimiento de UPS y grupo electrógeno en caso de presentarse una interrupción brusca de la energía eléctrica
		A.9.2.3 Seguridad e el cableado	Si Aplica	Se propone migrar el cableado (de datos y eléctrico) a un cableado de mejor categoría
		A.9.2.4 Mantenimiento de equipos	Si Aplica	Se redactará un documento detallando los mantenimientos periódicos de los equipos brindando una garantía en su uso
		A.9.2.6 Seguridad en el re-uso o eliminación de equipos	Si Aplica	Se retiran los equipos cuando ya se encuentras muy gastados o sin uso.

		A.9.2.7 Retiro de propiedad	Si Aplica	Se tienen identificadas a las personas y proveedores que retirarán los activos de la entidad bancaria
8	A.10.1 Procedimientos y responsabilidades de operación	A.10.1.2 Gestión de cambios	Si Aplica	Se redactará un documento detallando los responsables de los cambios en las gestiones de la entidad bancaria
		A.10.1.1 Documentación de procedimientos operativos	Si Aplica	Los colaboradores tendrán conocimiento que en el intranet de la entidad bancaria se encontrarán publicados los procedimientos para sus operaciones específicas
9	A.10.4 Protección contra software malicioso	A.10.4.1 Controles contra software malicioso	Si Aplica	La entidad bancaria cuenta con equipos protegidos frente a softwares maliciosos
10	A.10.7 Utilización y seguridad de los medios de información	A.10.7.3 Procedimientos de manipulación de la información	Si Aplica	Se establecerán procedimientos para la manipulación y almacenamiento de la información con el objetivo de proteger esta información frente a usos no autorizados
		A.10.7.4 Seguridad de la documentación de sistemas	Si Aplica	Se deberá proteger la documentación de los sistemas contra accesos no autorizados
11	A.10.8 Intercambio de información	A.10.8.1 Políticas y procedimientos para el intercambio de información	Si Aplica	En las políticas de seguridad de información se establecerá la manera de cómo se realiza el intercambio de información entre colaboradores o terceros
		A.10.8.4 Seguridad del correo electrónico	Si Aplica	Se deberá proteger la mensajería del correo electrónico (Ej. Mensajes encriptados)
12	A.11.1 Requisitos de negocio para el control de accesos	A.11.1.1 Política de control de accesos	Si Aplica	Se establecerá una política en la cual se eliminen todos los accesos de un colaborador al término de su vínculo laboral con la entidad bancaria
13	A.11.2 Gestión de acceso de usuarios	A.11.2.2 Gestión de privilegios	Si Aplica	Se establecerá políticas para restringir y controlar la asignación y uso de privilegios

		A.11.2.3 Gestión de contraseñas de usuario	Si Aplica	Se informará a los usuarios del formato de las contraseñas y la asignación que tienen cada uno mediante un proceso de gestión formal
14	A.11.3 Responsabilidades de los usuarios	A.11.3.1 Uso de contraseñas	Si Aplica	Se le exigirá al usuario el uso de buenas prácticas de seguridad en la selección y uso de las contraseñas
		A.11.3.3 Política de pantalla y escritorio limpio	Si Aplica	Se le exigirá al usuario sobre el escritorio limpio que debe mantener en su posición
15	A.11.4 Control de acceso a la red	A.11.4.2 Autenticación de usuarios para conexiones externas	Si Aplica	Se deberán utilizar métodos de autenticación adecuados para el control del acceso remoto
16	A.12.2 Proceso correcto en aplicaciones	A.12.2.1. Validación de los datos de entrada	Si Aplica	En la propuesta se redactan las aplicaciones para garantizar que los datos de entrada son correctos y apropiados
		A.12.2.4 Validación de los datos de salida	Si Aplica	En la propuesta se redactan las aplicaciones para garantizar que los datos de salida son correctos y apropiados

Fuente: Elaboración Propia

IV.3. Verificar (*Check*)

La evaluación y medición del desempeño de lo diseñado quedó a cargo de un responsable de seguridad de información de la entidad bancaria así como se diseñó una auditoría para su monitoreo en los procesos donde se implementó el SGSI.

A. Monitoreo, medición, análisis y evaluación

La entidad bancaria evaluará el desempeño de la seguridad de la información implantado en los procesos seleccionados en sus sedes principales y la eficacia de dicha herramienta.

Para ello se determina:

- A qué se necesita hacerle seguimiento, qué es necesario medir, sin olvidar incluir procesos y controles de la seguridad de la información.
- Las técnicas de seguimiento, medición, análisis y evaluación requeridas para garantizar que los resultados son válidos.
- Cuándo se ha de ejecutar tanto el seguimiento como la medición.
- Quien es el responsable de la ejecución del seguimiento y medición.
- Quién será el responsable de analizar y evaluar dichos resultados.

B. Auditoría interna

La auditoría permitirá identificar el nivel de cumplimiento del Sistema de gestión de seguridad de la información en las 6 sedes principales de la entidad bancaria con respecto a los controles y cláusulas de la norma internacional ISO 27001:2005, el cual se debe realizar un informe detallando lo siguiente:

1. **Alcance de la auditoría:** El alcance del SGSI está definido como: “Sistemas de información en los procesos *core* de la organización”.

2. **Fecha de la auditoría:** Las actividades de la auditoría serán ejecutadas 30 días después de haber implementado el SGSI, con una duración de 10 días laborables.

3. **Lugar:** La auditoría del SGSI se realizará en las 6 sedes principales de la entidad bancaria, incluyendo visitas a los centros de cómputo (*datacenter*, CCTV).
4. **Áreas auditadas:** Se auditarán todas las áreas de las 6 sedes principales de la entidad bancaria que están relacionadas con los procesos del alcance del SGSI, es decir, áreas Administrativas, Sistemas, *call center*, Tecnologías de la Información, Operaciones, Infraestructura, Helpdesk y Seguridad y Accesos.

5. **Equipo auditor:** La auditoría será ejecutada por el oficial de seguridad de la información del banco como auditor interno y un equipo proveedor de seguridad de la información como auditores externos.

6. **Personal auditado:** Serán todos los participantes que están involucrados en los procesos en el alcance del SGSI.

7. **Hallazgos de la auditoría:** Son los resultados de haber realizado la auditoría externa, donde incluye el tipo de hallazgo, el control según la norma ISO 27001:2005, descripción de lo encontrado y la criticidad del hallazgo.

8. **Conclusiones:** Enunciados sobre el estado final de la auditoría realizada.

Tabla V.3.1
Plan de auditoría del SGSI en la organización

Plan de auditoría Sistema de Gestión de Seguridad de la Información				
Ítem	**Nombre de la tarea**	**Duración (DL)**	**Inicio**	**Finalizar**
1	**Plan de auditoría Sistema de Gestión de Seguridad de Información**	45	30/10/17	22/12/17
2	**Conformación del equipo de trabajo auditor**	1	30/10/17	30/10/17
3	**Inicio de la auditoría**			
3.1	Presentación del proyecto	1	01/11/17	01/11/17
3.2	Firma del acta de inicio por gerencia	1	02/11/17	02/11/17
4	**Planificación**			
4.1	Reunión con el equipo de trabajo (auditores y auditados) y definición alcance	2	03/11/17	04/11/17
4.2	Creación/ajuste del cronograma de auditoría	2	07/11/17	08/11/17

4.3	Documentación de las pruebas	3	09/11/17	11/11/17
4.4	Entrega del cronograma ajustado para su aprobación	1	14/11/17	14/11/17
5	**Pruebas**			
5.1	Recolección de información			
5.1.1	Entorno interno, procesos y personal	2	15/11/17	16/11/17
5.1.2	Estudio de información recolectada	3	17/11/17	21/11/17
5.2	Ejecución de la pruebas			
5.2.1	Revisión de actas, acuerdos y conformación del SGSI	2	22/11/17	23/11/17
5.2.3	Revisión de informes de riesgos y políticas	2	24/11/17	25/11/17
5.2.4	Revisión de controles ISO/IEC 27001 implementados	2	28/11/17	29/11/17
5.2.5	Revisión de condiciones técnicas y casos de uso	3	30/11/17	01/12/17
5.2.6	Ejecución técnica de pruebas: Análisis de vulnerabilidades y amenazas	2	04/12/17	05/12/17
5.2.7	Entrega de informes preliminares	1	06/12/17	06/12/17
5.3	Análisis de la documentación			
5.3.1	Revisión de documentación	2	07/12/17	08/12/17
5.3.2	Ejecución de entrevistas y visitas	3	08/12/17	11/12/17
5.3.3	Pruebas técnicas: Análisis de vulnerabilidades	2	12/12/17	13/12/17
5.3.4	Reunión de seguimiento de auditoría	1	14/12/17	14/12/17
5.4	Elaboración de informes	3	15/12/17	18/12/17
5.5	Presentación de informes	1	19/12/17	19/12/17
5.6	Cierre de auditoría			
5.6.1	Generación de informe de cierre	3	20/12/17	21/12/17
5.6.2	Generación de cronograma de revisión anual/semestral del SGSI	2	22/12/17	22/12/17

Fuente: elaboración Propia

C. Revisión por la Alta Dirección

El objetivo es redactar un informe donde se establezca los lineamientos para que la Alta Dirección revise el Sistema de gestión de Seguridad de la Información y asegurar continuamente que se cumplan todos los protocolos, requisitos, controles y normas con eficiencia y efectividad, este informe debe contener lo siguiente:

1. **Alcance:** En el informe se redactará el Sistema de Gestión de Seguridad de la Información en su conjunto, ya que se trata de una revisión global de los aspectos que son de interés para evaluar el funcionamiento del mismo.

2. **Responsabilidades:** La Alta Dirección es la encargada de efectuar la revisión por la gerencia o dirección, aunque puede delegar las funciones operativas de este procedimiento a terceros (profesionales en seguridad de la información). El comité de seguridad de la información que serán los encargados de mantener la operatividad del SGSI en los procesos seleccionados.

3. **Diagrama de flujo:** Donde se demuestra o se desarrolla paso a paso la revisión del informe donde se involucra a los participantes encargados de la seguridad de la información.

4. **Revisión:** Se debe contar con la siguiente información:
   - Resultados de auditorías (internas y/o externas).
   - Desempeño de los procesos y conformidad del producto.
   - Estado de las acciones correctivas y preventivas.
   - Acciones de seguimiento de las revisiones hechas por la Alta Dirección.
   - Cambios que podrían afectar o favorecer al SGSI.
   - Recomendaciones para la mejora.

5. **Evaluación y análisis de resultados:** Una vez extraída la información posible, se analiza teniendo en cuenta los objetivos y la política de la entidad bancaria, en busca de acciones correctivas y preventivas y dar oportunidades para la mejora del desempeño.

6. **Toma de decisión de acciones y aprobación:** El análisis realizado en la fase anterior puede concretarse en: observaciones, modificaciones y/o objetivos para el SGSI, así como comentarios generales sobre la evolución del mismo. Las conclusiones alcanzadas pueden dar lugar a acciones dirigidas a la mejora en las entidades bancarias, en función de los recursos disponibles. Si esto ocurre, la alta dirección es la encargada de aprobarlas para su implementación, previa consideración de su viabilidad económica y técnica.

7. **Asignación de responsables y seguimiento de acciones:** Se establecen los responsables más apropiados para emprender las acciones de acuerdo al rol que se le asignaron a cada uno. Durante la puesta en marcha de las

acciones, se llevará a cabo un seguimiento de su mejora. En la siguiente revisión por la Dirección que se realice, esta información servirá para evaluar si los problemas detectados en la sesión anterior vuelven a presentarse, si las acciones emprendidas fueron (o están siendo) apropiadas y si los usuarios están satisfechos

IV.4. Actuar (*Act*)

Este último punto del modelo Deming se toman acciones correctivas y preventivas de acuerdo a los resultados del Sistema de Gestión de Seguridad de la Información implementado, la revisión y aprobación de esta herramienta es responsabilidad de la Alta Gerencia como las gerencias de las áreas involucradas. La implementación y el mejoramiento continuo de esta herramienta, estará bajo el cargo de las áreas de Seguridad de la información, infraestructura de TI, Networking o una empresa tercera que se encargue de mantener y mejorar los puntos establecidos en el diseño del proyecto y los hallazgos encontrados.

Una vez aprobado, la Alta Gerencia demostrará su compromiso a través de:

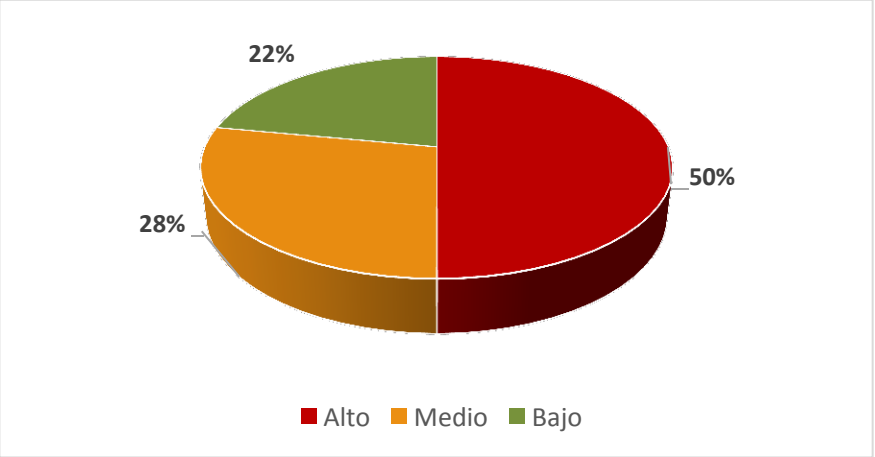
- La revisión y aprobación de las políticas de seguridad de la información.
- La promoción activa de una cultura de seguridad dentro de la compañía.
- Facilitar la divulgación del manual de seguridad a todos los colaboradores de la empresa según el nivel de seguridad que les corresponde.
- Asegurar los recursos adecuados para implantar y mantener las políticas y el Sistema de Gestión de la Seguridad de la Información.

IV.5. Análisis de resultados:

A. Con respecto al riesgo:

En las encuestas realizadas se preguntaron a los 351 usuarios temas sobre Tecnologías de información, Ambientes, Empresa, Seguridad del ordenador, Información personal y Seguridad general obteniendo como resultado de los niveles de riesgo mostrado en el siguiente gráfico:

Gráfico V.7
Nivel del riesgo de los activos en la encuesta

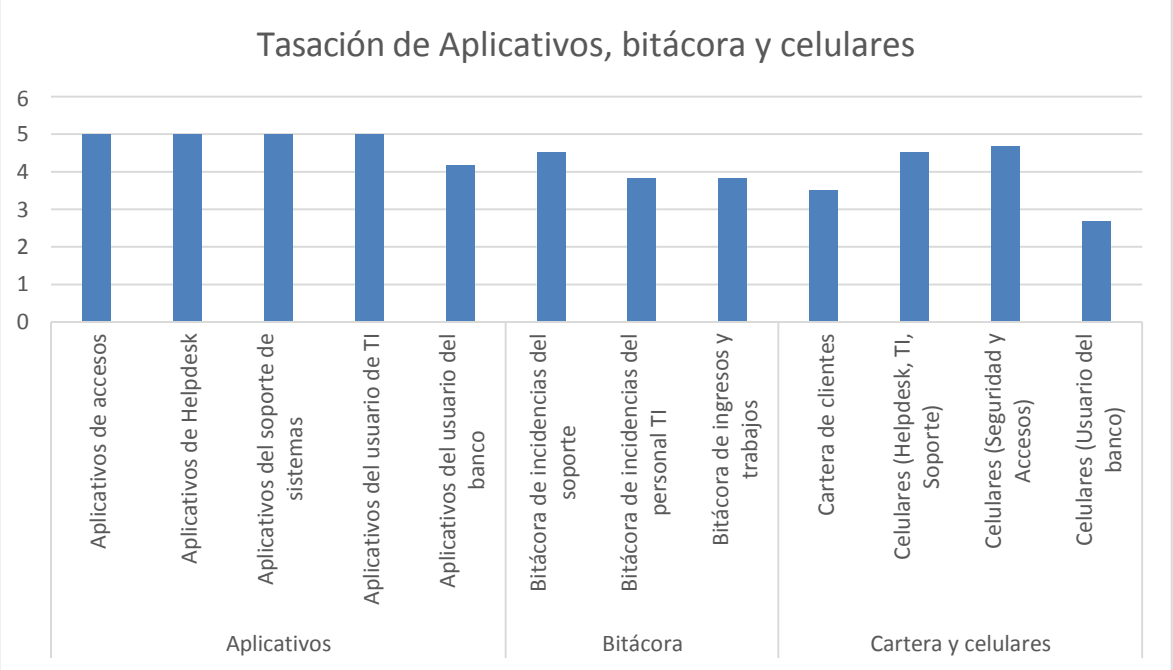


Fuente: Elaboración propia

B. Con respecto a la tasación de los activos de información

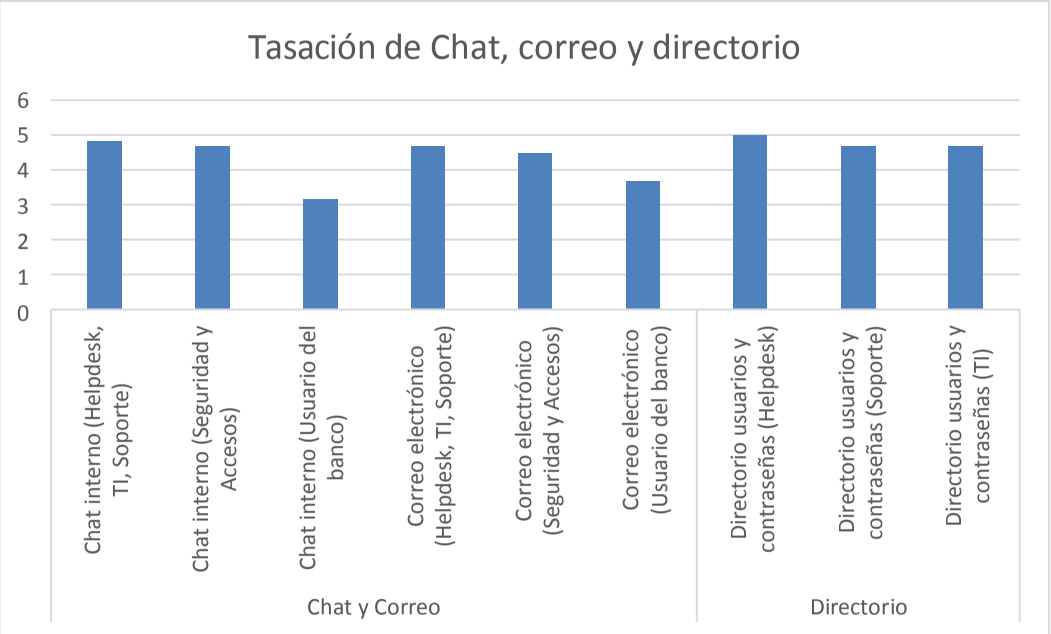
Se utilizó la escala de Likert para determinar del valor del activo frente a la pérdida o falla que afecte la confidencialidad, disponibilidad e integridad del activo de información tomando como promedio los pilares de la seguridad mostrados en los siguientes gráficos:

Gráfico V.8
Tasación de Aplicativos, bitácora y celulares



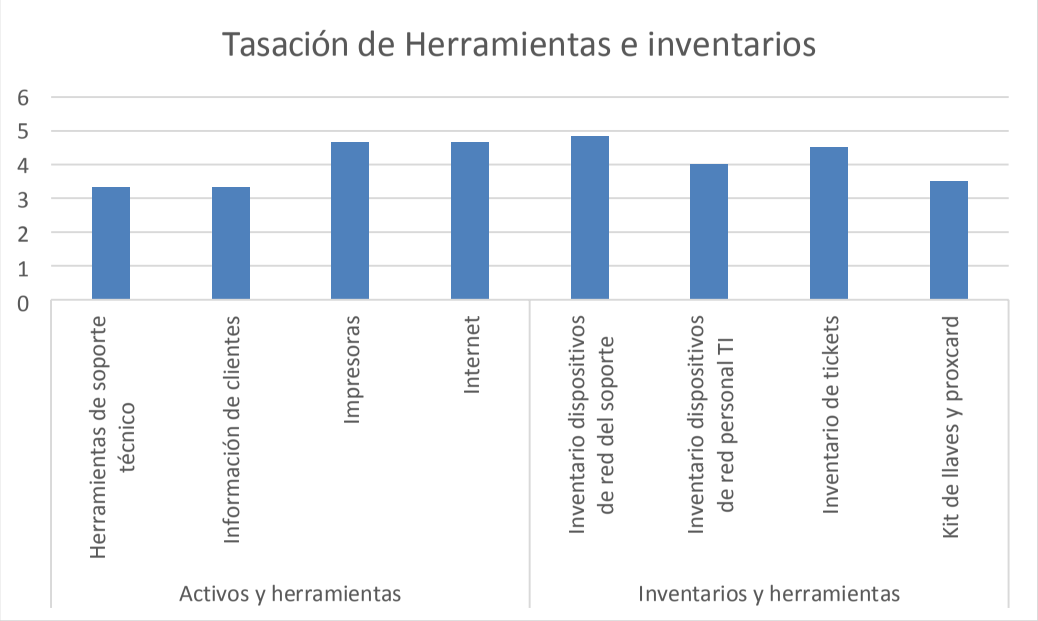
Fuente: Elaboración propia

Gráfico V.9
Tasación de Chat, correo y directorio



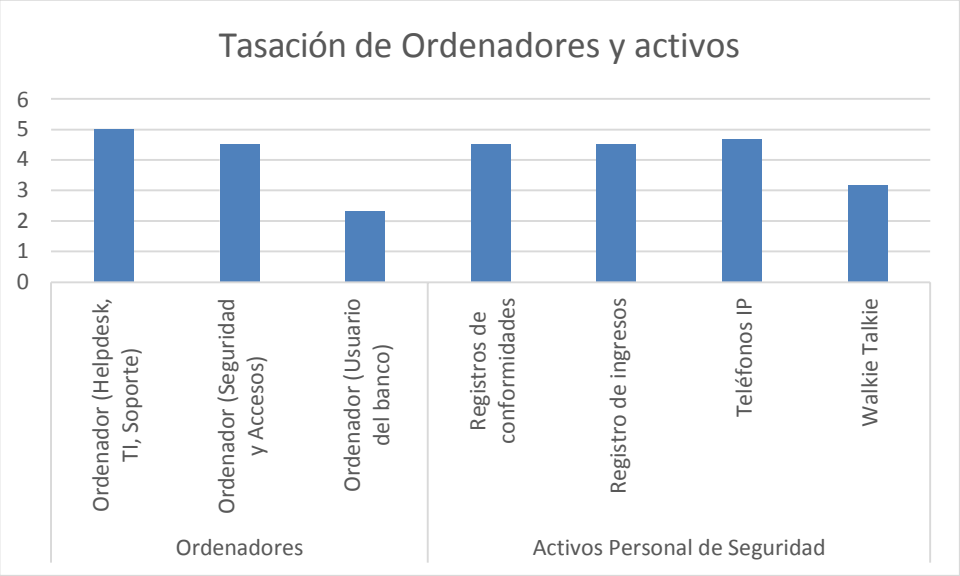
Fuente: Elaboración propia

Gráfico V.10
Tasación de Herramientas e Inventarios



Fuente: Elaboración propia

Gráfico V.11
Tasación de Ordenadores y activos



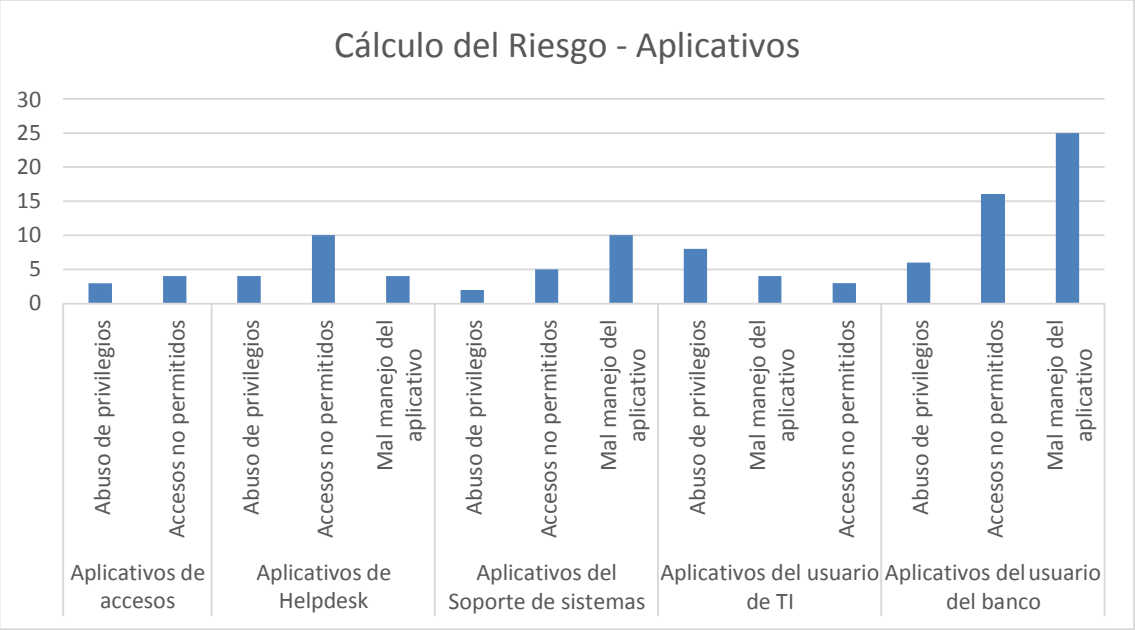
Fuente: Elaboración propia

Con esto observamos que los niveles más bajos, en promedios, en cuanto a confidencialidad, disponibilidad e integridad vienen por parte de los usuarios de banca por teléfono (como en el uso de los aplicativos, bitácora, el uso de los celulares, sus ordenadores, uso del chat, correo y directorio) puesto que no cuentan con capacitaciones o fuente de información que les permita conocer la protección o cuidado de sus activos.

C. Con respecto a las Amenazas, Vulnerabilidades y el Cálculo del Riesgo

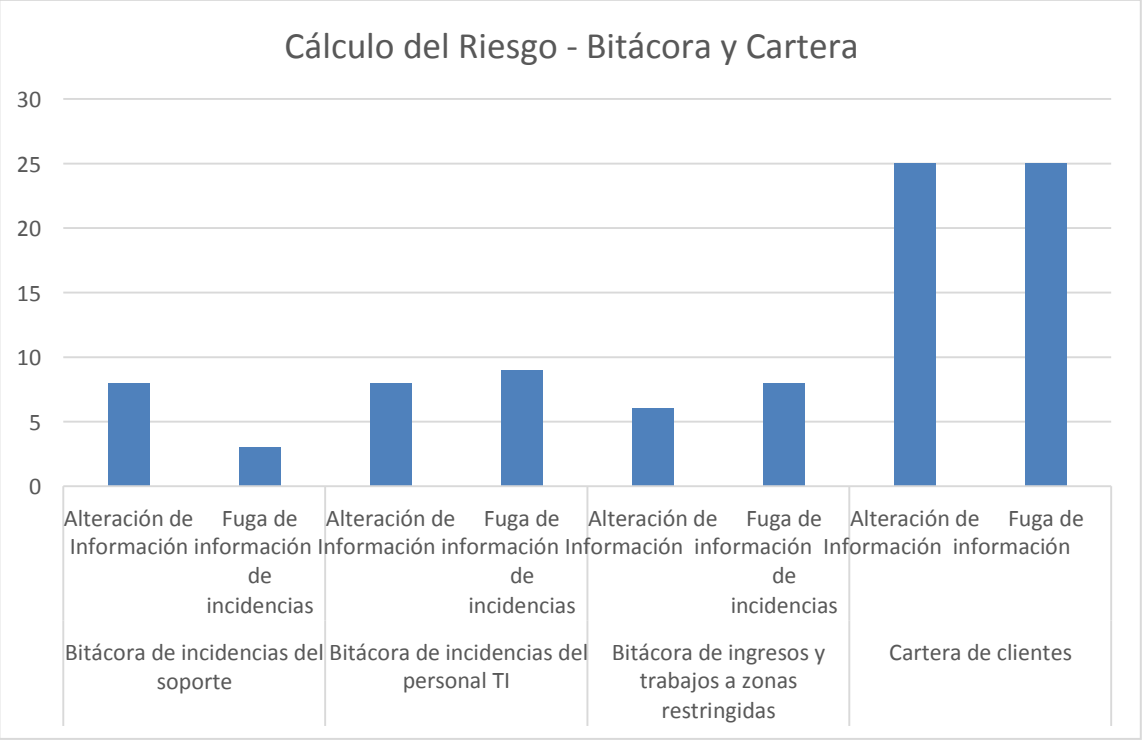
Se identificaron las amenazas y vulnerabilidades que presentan los activos de información, luego de ello se determinó la posibilidad de ocurrencia que ambos presentan como también impacto para obtener el cálculo del riesgo al que está expuesto el activo de información. La escala que se utiliza es en base al cálculo del riesgo, obteniendo como resultado del Impacto por la Probabilidad de ocurrencia.

Gráfico V.12
Cálculo del Riesgo - Aplicativos



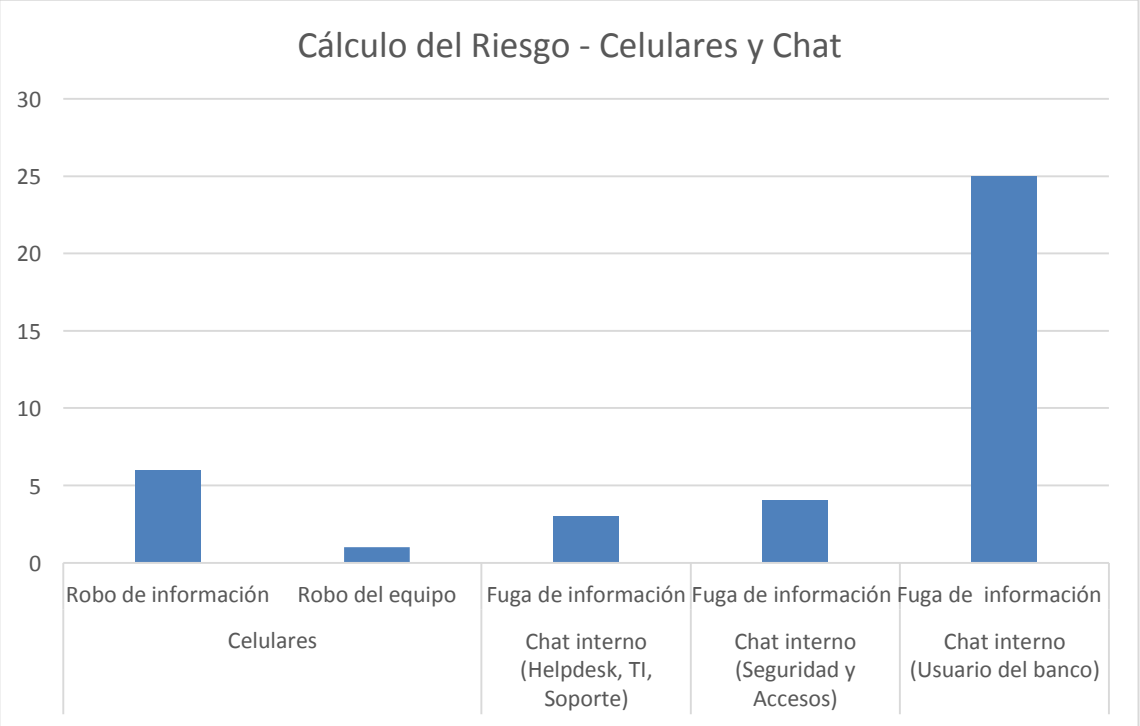
Fuente: Elaboración propia

Gráfico V.13
Cálculo del Riesgo – Bitácora y Cartera



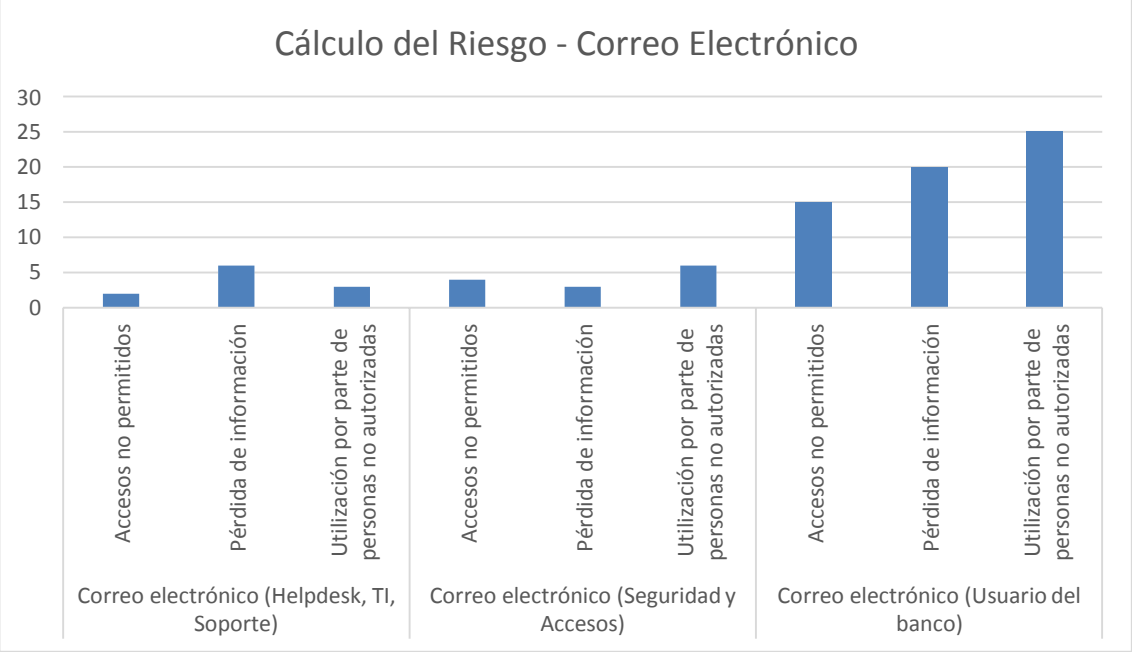
Fuente: Elaboración Propia

Gráfico V.14
Cálculo del Riesgo – Celulares y Chat



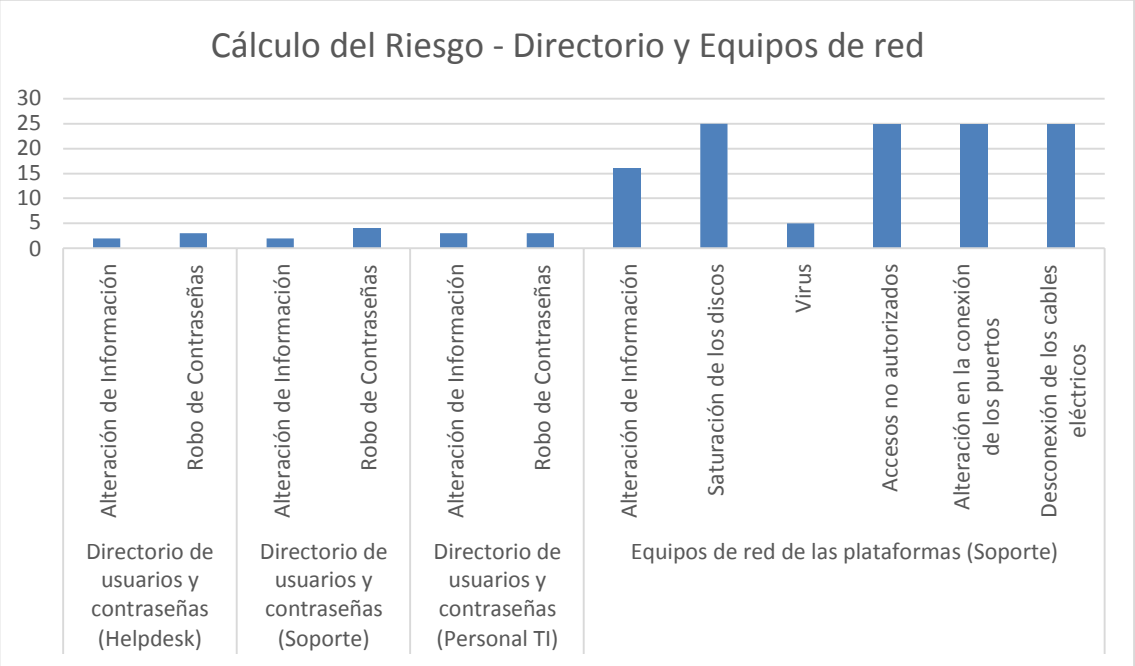
Fuente: Elaboración propia

Gráfico V.15
Cálculo del Riesgo - Correo Electrónico



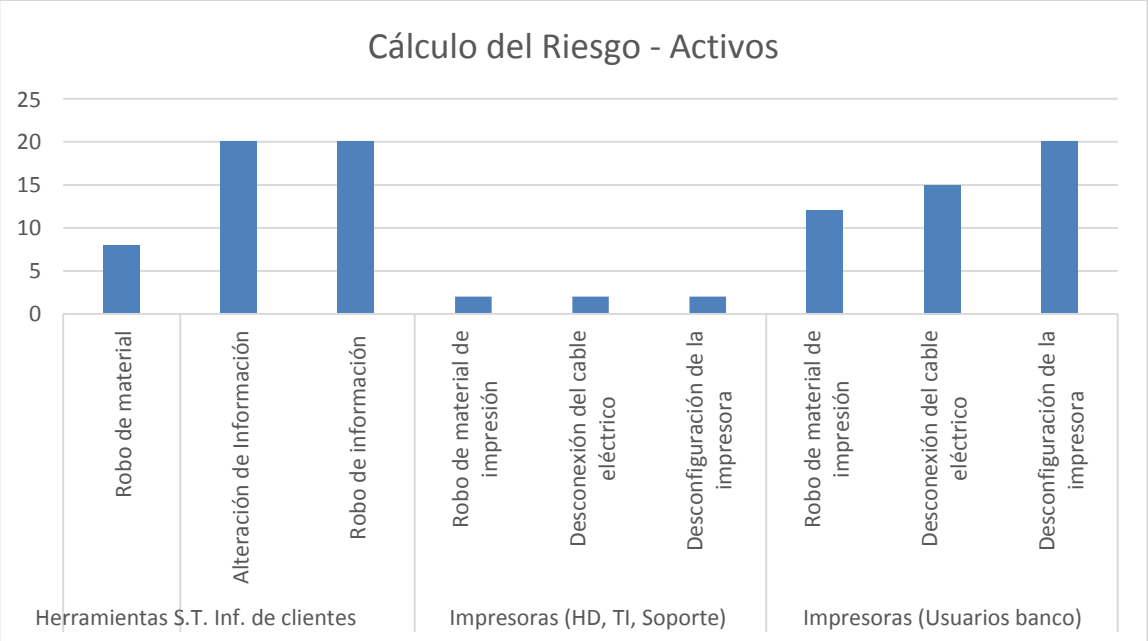
Fuente: Elaboración propia

Gráfico V.16
Cálculo del Riesgo - Directorio y equipos de red



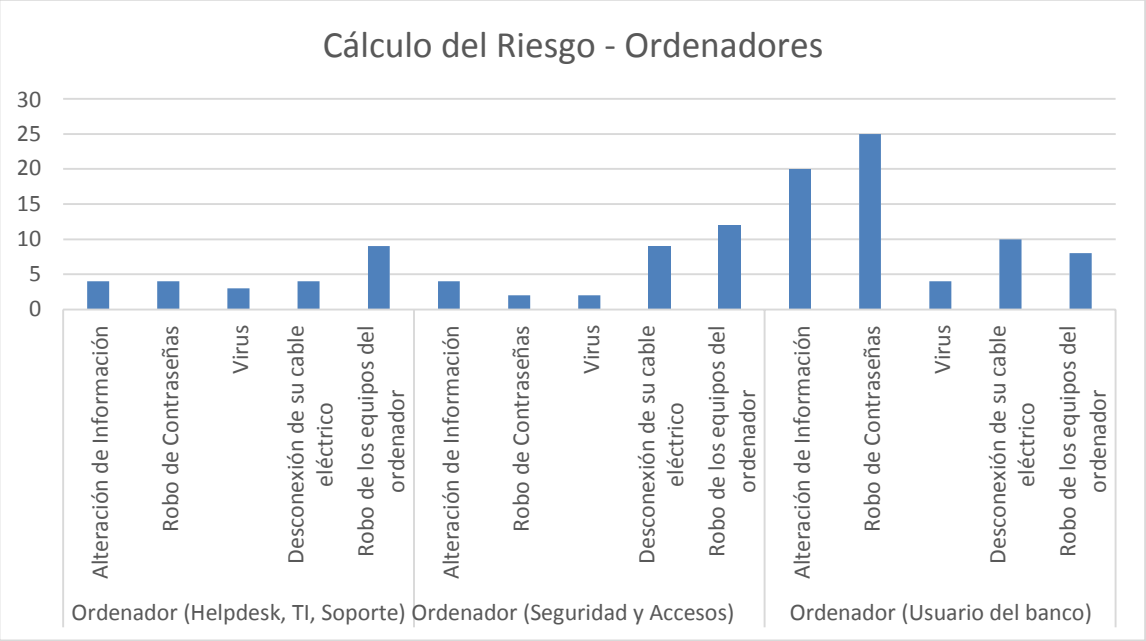
Fuente: Elaboración propia

Gráfico V.17
Cálculo del Riesgo - Activos varios



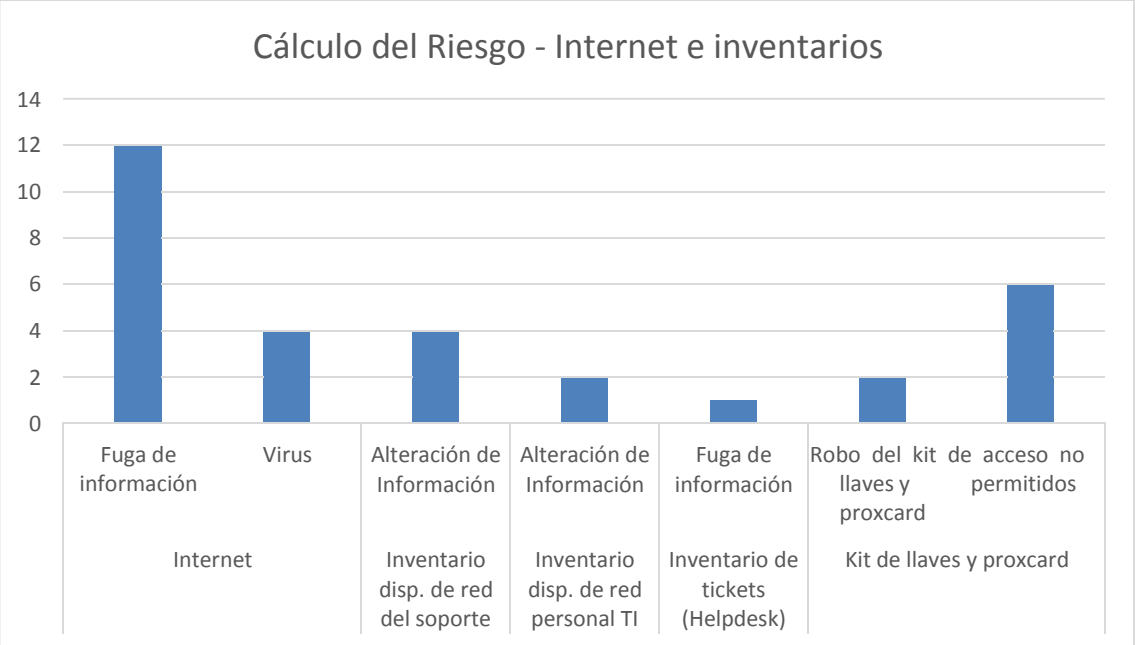
Fuente: Elaboración propia

Gráfico V.18
Cálculo del Riesgo - Ordenadores



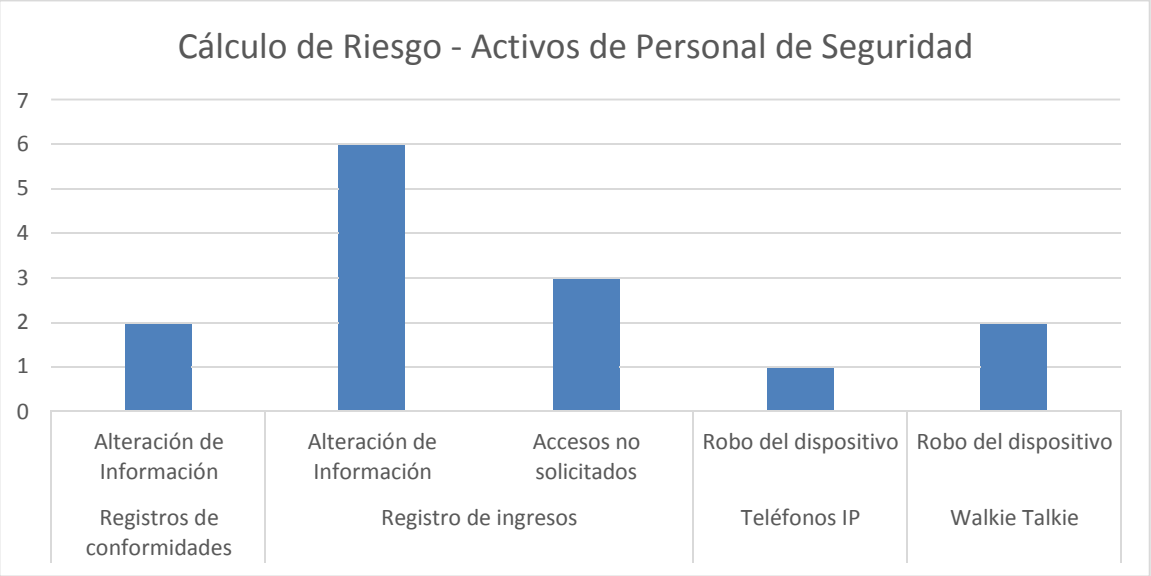
Fuente: Elaboración propia

Gráfico V.19
Cálculo del Riesgo - Internet e Inventarios



Fuente: Elaboración propia

Gráfico V.20
Cálculo del Riesgo - Activos Personal Seguridad



Fuente: Elaboración propia

D. Con respecto a la Evaluación del Riesgo

Del hallazgo obtenido en el diseño en cuanto a los riesgos en los activos de información se determinaron cuáles son los que la entidad financiera está dispuesta a asumir, aceptar y mitigar así como también los que serán transferidos a una empresa tercera, como por ejemplo:

D.1. Equipos de red: La saturación de los discos, conexiones de red, virus o accesos no autorizados son riesgos de los cuales los asumirá la organización y la gestión de los riesgos será transferido a una empresa tercera, las empresas propuestas en el diseño son Xentic Perú, Fortinet Perú, SGS Del Perú, HackSoft SAC y Secure Soft.

D.2. En cuanto al robo de activos se incrementará la cantidad de cámaras de vigilancia instaladas en los ambientes de los usuarios del banco que serán controlados por un Circuito Cerrado de Televisión (CCTV) a cargo de personal de la empresa G4S Perú (empresa de seguridad propuesta en el diseño).

D.3. Los riesgos como las desconexiones eléctricas de equipos o desconfiguraciones, así como la alteración de la información en el inventario de tickets de Helpdesk lo asumirá el área de Infraestructura de TI y la gestión de los riesgos será responsabilidad de una empresa tercera, empresas como Sodexo Perú, SGT Telecomunicaciones, CTI

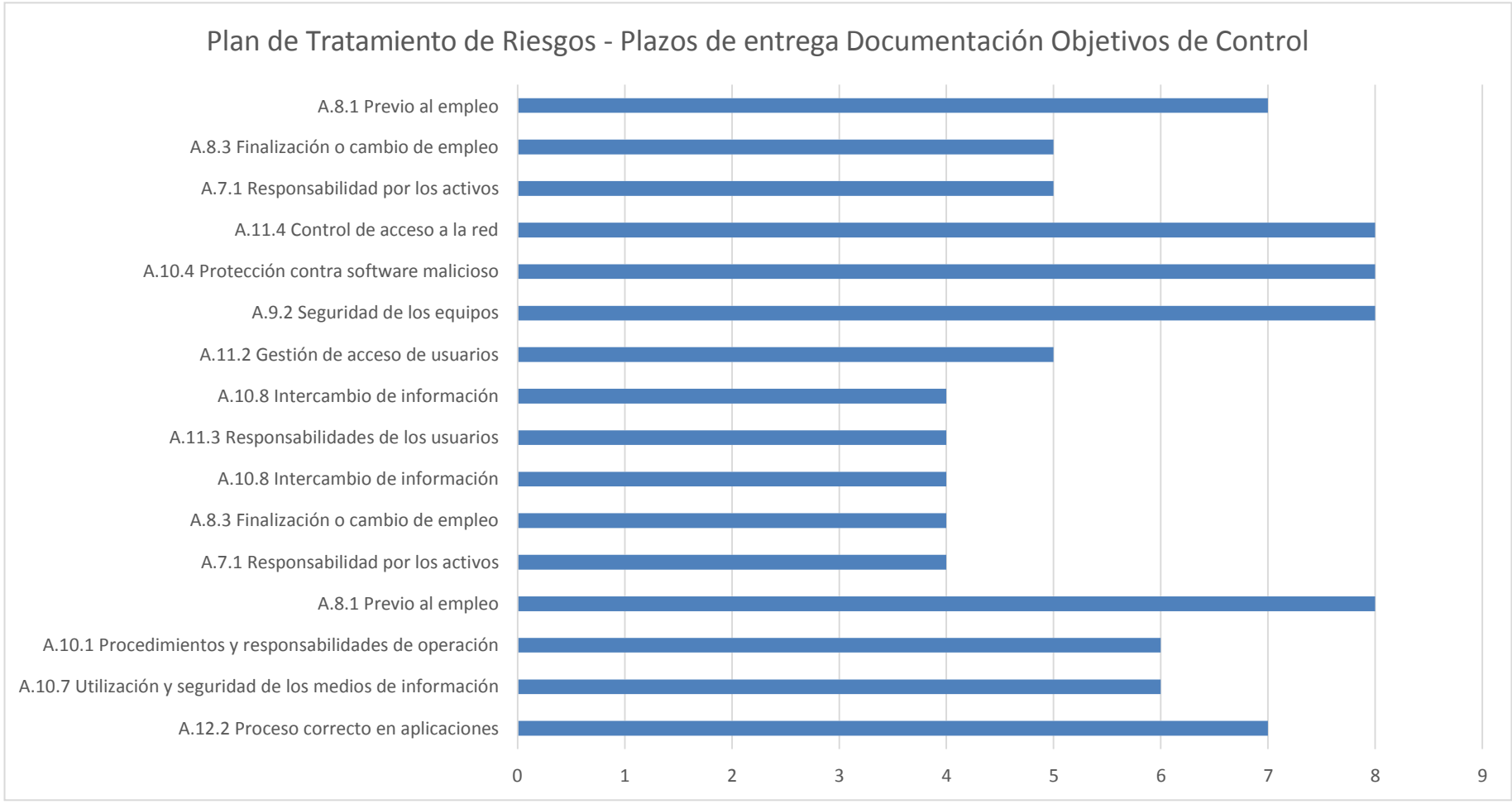
Enterprise, Yellec SAC, Italtel Perú., con el fin de tener un control ante estos cambios y evitar más adelante una posibilidad de ocurrencia.

D.4. En cuanto a la pérdida de información, uso de aplicativos, registro de bitácora, cartera de clientes y ordenadores, la organización se apoyará en la implementación del Sistema de Gestión de Seguridad de Información con el fin de mitigar los riesgos encontrados en el diseño.

E. Con respecto al Plan de Tratamiento de Riesgo

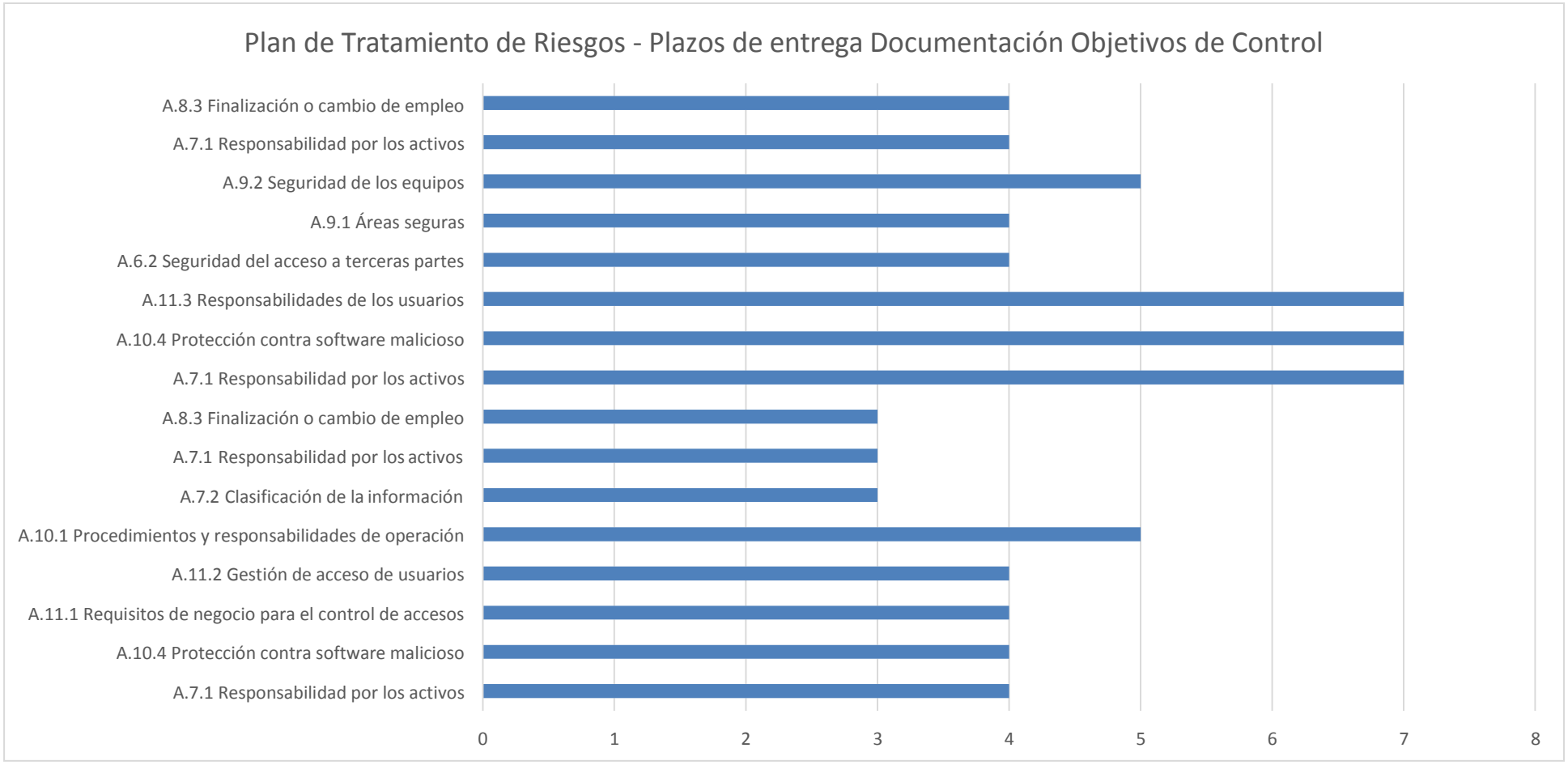
En los siguientes gráficos se muestran los plazos de entrega (en días) por cada objetivo de control documentado (en formato .pdf y .docx a la Alta gerencia como a las gerencias involucradas en el proyecto) de acuerdo a los controles establecidos para cada activo de información tal como se detalla en la tabla V.2.6.

Gráfico V.21
Plan de Tratamiento de Riesgos - Documentación Objetivos de Control (Plazos de Entrega en días)



Fuente: Elaboración propia

Gráfico V.22
Plan de Tratamiento de Riesgos - Documentación Objetivos de Control (Plazos de Entrega en días)



Fuente: Elaboración propia

V. DISCUSIÓN Y CONCLUSIONES

V.1. Discusión

De la investigación, resultados de la encuesta nos permitió saber qué tan crítico se encuentran los niveles de riesgo en las seis sedes de la entidad bancaria, ello responde a que se presentan 50% en nivel de riesgo alto, 28% en nivel de riesgo bajo y 22% como nivel de riesgo bajo, este estudio determinó que son los usuarios de atención al cliente y de banca por teléfono los que presentan estos niveles de riesgos en las sedes de la organización.

La tabla de amenazas y vulnerabilidades se clasificaron por áreas según sus activos de información (esto se enmarca en lo descrito por ISACA 2016, donde establece que los riesgos deben necesariamente tener una respuesta de la alta dirección como referencia los umbrales de riesgo) donde los riesgos altos como el manejo de los aplicativos, accesos no permitidos y fuga de información tienen una valoración de cálculo del riesgo de 16 a 25, ocasionando un impacto alto en los activos de información.

Estos riesgos encontrados en la fase del cálculo se evaluaron con el fin de identificar cuáles se van a mitigar, transferir o evitar bajo el uso de la herramienta del Sistema de Gestión de Seguridad de la Información, como son los virus, fuga de información, robos de ordenadores y dispositivos (proceso para transferir), alteración y robo de información, saturación de discos duros (proceso de mitigar), etc., puesto que una vez identificados se propone a la alta gerencia la implementación de esta herramienta de seguridad lo cual permitirá reducir los riesgos existentes en la organización y la alta dirección puede decidir cuál será su respuesta, según el apetito de riesgo de la organización en cuanto a aceptar, mitigar, evitar o transferir.

La coordinación, respuesta y aprobación de la alta dirección conlleva que se diseñe e implemente el plan de tratamiento de riesgos en cuanto a los plazos de entrega de acuerdo a los objetivos de control y sus controles (como La Seguridad del acceso y equipos, Responsabilidad y clasificación de los activos, finalización del empleo, Seguridad de los equipos, responsabilidades de los usuarios etc.) como también la presentación el costo total del proyecto que asciende a 200082 dólares americanos y el tiempo de ejecución de los proyectos involucrados en la seguridad de la información.

Del estudio realizado, los usuarios de Banca por Teléfono son los que tienen niveles de riesgo altos, puesto que la mayoría de ellos no cuentan con

conocimientos o capacitaciones en seguridad de la información, las capacitaciones permitirán tener una concientización sobre sus activos al estar expuesto a riesgos que adulteren su integridad, esta actividad se encuentra dentro de la propuesta y será auditada como cumplimiento de la investigación.

Además, se realizará auditoría de manera periódica y en las fechas establecidas por la investigación el cual fortalecerá el cumplimiento de todas las actividades de la gestión de seguridad permitiendo mantener un nivel de riesgo bajo y preservar la seguridad de los activos.

Así mismo, para que la gestión de seguridad de la información de los activos pueda ser implementada y mantenida en el tiempo, es muy importante contar con el tema económico, pues permitirá contar con personal especializado (un oficial de seguridad de la información externo o de la organización), con un buen equipamiento de hardware y lo más actualizado en software puesto que se encontraron equipos de red, antivirus y programas que no están actualizados en sus últimas versiones, como por ejemplo el Microsoft Office, NOD32 antivirus, aplicaciones de usuarios, etc., y de no contar con las versiones requeridas se genera una brecha permitiendo a los delincuentes informáticos adulterar o robar la información.

Finalmente, el factor humano es crítico e importante para la implementación y sobre todo para el mantenimiento del nivel óptimo de la seguridad en la organización, por tanto, todo el personal (mencionado en la investigación) debe participar en las auditorías y aplicar los conocimientos sobre la seguridad de la información para mantener bajo los niveles del riesgo.

V.2. Conclusiones

La investigación desarrollada en seis sedes de una entidad bancaria del Perú determinó la manera cómo un Sistema de Gestión de Seguridad de la Información cuantifica los riesgos de la seguridad de la información, lo cual se evidencia en:

A. Se diseñó un Sistema de Gestión de Seguridad de la Información en seis sedes de una entidad bancaria del Perú, demostrando con esta propuesta la cuantificación de los riesgos de información que resultó hacer el estudio en las seis sedes de la entidad bancaria, encontrando a un 50% el nivel de riesgo alto, 28% riesgo medio y 22% el riesgo bajo en los usuarios como en los equipamientos de los equipos en las áreas.

B. Se evaluó el proceso de gestión de riesgos en las seis sedes de una entidad bancaria del Perú con la identificación de los activos, amenazas y vulnerabilidades que nos ayudaron a encontrar los niveles de riesgo existentes en la organización a través de la Evaluación y Cálculo del riesgo, niveles altos de riesgos frente a las amenazas como en el robo de información en la cartera de clientes, celulares, chat, correo, como también los accesos no autorizados, virus, cableado de equipos y robo en los equipos de comunicación de red, etc., el cual se describe en la tabla V.2.5 Evaluación del riesgo por activo de información, donde se detalla cuáles se van a mitigar, transferir, aceptar y evitar puesto que los niveles de riesgo alto están en un 50% de impacto en la organización.

C. Se identificó las brechas existentes de seguridad, el uso de la herramienta sistema de gestión de seguridad de la información determinó que solo se tiene un 30% de cumplimiento en la seguridad de la información de las sedes de la entidad bancaria, siendo los usuarios de Banca por Teléfono los que menos cumplen con los objetivos y políticas de seguridad por falta de concientización y capacitaciones que no cuenta la organización en sus objetivos para preservar la seguridad.

D. Se seleccionaron los controles y objetivos de control de la seguridad de la información en las seis sedes de una entidad bancaria del Perú por el uso del Sistema de Gestión de Seguridad de la Información, con la versión de la norma ISO 27001:2005 los objetivos y controles como propuesta a implementarse corresponden a las cláusulas de Seguridad Organizacional,, Gestión de activos, Seguridad en los recursos humanos, Seguridad física, Gestión de comunicaciones, Control de accesos, etc., aplicados según la tabla V.2.9: Declaración de aplicabilidad del SGSI, objetivos de control y controles por la que serán mantenidos, ejecutados y auditados bajo la aprobación de la Alta dirección por la misma entidad o por un tercero.

VI. RECOMENDACIONES

VI.1. El Sistema de Gestión de Seguridad de la Información diseñado para las seis sedes de una entidad bancaria del Perú, debe ser implementado para mantener la cuantificación de los riesgos de seguridad existentes en activos para preservar la confidencialidad, integridad y disponibilidad de los activos de información frente a los niveles de riesgos encontrados en el diseño.

VI.2. Contar con la Gestión del riesgo (documentado con la Evaluación y Cálculo del riesgo) para tener una adecuada identificación de las amenazas y vulnerabilidades en los activos, la toma de decisiones y evitar que ocurran riesgos que impacten en la seguridad de la información bajo un responsable de la entidad bancaria o un tercero.

VI.3. Implementar el Sistema de Gestión de seguridad de información para reducir las brechas existentes y aumentar el porcentaje de cumplimiento de la seguridad en la información, así como capacitar de manera periódica a todo el personal involucrado (de manera especial a los usuarios de banca por teléfono) en los procesos seleccionados sobre seguridad de la información en las seis sedes de la entidad bancaria sobre las amenazas posibles o presentes como los virus, fuga de información, robos de ordenadores y dispositivos, alteración y robo de información, saturación de discos duros, etc.

VI.4. Implementar los controles y Objetivos de control que se determinaron en el diseño para gestionar eficientemente la seguridad de la información en las seis sedes de la entidad de bancaria, mantener una protección adecuada sobre los activos, la seguridad física, del entorno, así como la gestión adecuada de las operaciones, el control de los accesos y el mantenimiento de los sistemas con el fin de mantener bajo los niveles del riesgo.

VII. FUENTES DE REFERENCIA

VII.1. Laudon, Kenneth (2012) Sistemas de Información Gerencial. Pearson Educación de México S.A.

VII.2. ISO 27001 "ISO Survey 2015 Certificates". Disponible en: www.iso.org/iso/survey/iso_27001_iso_survey2015.xlsx

VII.3. ISO Tools Excellence "Las claves del éxito para la gestión de riesgos". Disponible en: www.isotools.org/Claves-del-exito-para-la-gestion-de-riesgos.pdf

VII.4. ISO Tools Excellence "La norma ISO 27001 Aspectos clave de su diseño e implantación". Disponible en: www.isotools.org/La-norma-ISO27001-aspectos-clave-de-su-diseño-e-implantación.pdf

VII.5. EY "Crear confianza en el mundo digital". Disponible en: http://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015.pdf

VII.6. Morelo, Alberto (2015), Elaboración de un plan de implementación de ISO/IEC 27001:2013.

VII.7. EDI. Sistemas de gestión de seguridad de la información – Especificaciones con guía de uso, NTP 821.101: 2005.

VII.8. José Manuel Fernández Domínguez (2006) Sistema de Gestión de Seguridad de la Información según ISO 27001:2005. Disponible en: http://www.nexusasesores.com/docs/ISO27001-norma-eimplantacion-SGSI.pdf.

VII.9. Alejandro Corletti Estrada (2006) ANÁLISIS DE ISO-27001:2005. Disponible en: http://www.mastermagazine.info/informes/9544.php.

VII.10. Fernández, Eduardo y Mario Piattini (2003) Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada. Primera edición. Madrid: Ediciones Aenor.

VII.11. García, Alfonso y María del Pilar Alegre (2011) Seguridad Informática. Primera edición. Madrid: Ediciones Paraninfo SA.

VII.12. Donado, Siler Amador y Flechas Andrés (2001) Seguridad Computacional. Primera edición, Editorial Cauca

VIII. ANEXOS

VIII.1. Anexo 1: Encuesta de seguridad de información

ENCUESTA DE RESPUESTA CERRADA	
Recolección de datos para realizar el estudio de la Seguridad de la Información de los centros de contacto de las entidades bancarias del sector nacional 2017	
Universidad Privada del Norte - Maestría en Gerencia de Sistemas de Información y Auditoría	
Entidad bancaria:	Encuesta anónima

Cantidad de usuarios encuestados	
Usuarios de línea bancaria	224
Sistemas y soporte	23
Helpdesk	49
Seguridad y Accesos	18
Operaciones TI	37

Tecnología de la Información	SI	NO	N/S
1. ¿Conoce qué antivirus tiene instalado en su ordenador?			
2. ¿Le brindan capacitaciones sobre ciberseguridad o seguridad de información?			
3. ¿cuenta con acceso a todas las páginas web que usted necesita acceder?			
4. ¿Cuenta con todos los aplicativos que usted necesita acceder?			
Ambientes	**SI**	**NO**	**N/S**
5. ¿Ha observado si usuarios o colaboradores de su área u otras áreas tienen su información expuesta en sus posiciones frente a todos los trabajadores de la empresa? (contraseñas, carteras de clientes, directorios, etc.).			
6. ¿Ha ingresado a ambientes físicos restringidos de su empresa?			
7. (Responder en caso la pregunta 6 es afirmativa), ¿Ingresó con una autorización por su jefe inmediato?			
8. ¿Su empresa le ofrece lockers o stands para guardar su información (libros, folders, documentos de clientes)?			
9. Los ambientes de operaciones, créditos, tecnología, ¿Cuentan con cámaras de vigilancia para asegurar que los activos no sean manipulados?			
Empresa	**SI**	**NO**	**N/S**
10. ¿Supo de algún fraude de dinero en su empresa por parte de un cliente o un colaborador?			
11. En la empresa donde labora, ¿se debe brindar información de un colaborador si el cliente lo solicita? (nombre, área, jefatura)			
12. Con usted mismo u otro colaborador, ¿Presenció algún robo dentro de la empresa?			
13. Responder en caso la pregunta 10 es afirmativa ¿informó su jefe inmediato?			
Seguridad del ordenador	**SI**	**NO**	**N/S**
14. ¿Se realiza un mantenimiento informático periódico sobre el ordenador donde trabaja?			

15. (Responder en caso la pregunta 14 es afirmativa), ¿Estuvo presente durante el mantenimiento informático observando que el encargado del trabajo no copie ni elimine su información?			
16. Si trabaja con ordenador portátil, ¿cuenta con un cable de seguridad o anclaje?			
17. Si trabaja con ordenador portátil, ¿cuenta con acceso wifi?			
18. (Responder en caso la pregunta 17 es afirmativa), ¿conoce si el acceso a wifi tiene medida de seguridad para proteger dicha conexión?			
Información personal	**SI**	**NO**	**N/S**
19. ¿Tiene un respaldo o backup de su información en caso ocurra un desastre natural, robo o eliminación de información?			
20. ¿Está autorizado por su jefatura en descargar archivos o información de su trabajo en su ordenador y copiarlo a un disco externo como un usb?			
21. (Responder en caso la pregunta 20 es negativa), ¿Descargó o copió archivos a su disco externo por adquirir tal información?			
22. El almacenamiento de sus correos, datos, información, ¿se conecta a través de una ruta compartida hacia otro ordenador?			
23. Colaborador de la empresa o proveedor, ¿conoce la contraseña de su computadora o usuario?			
24. ¿Le ha ocurrido un robo de sus activos en su sitio de trabajo? (Celular, documentos, llaves, dinero, etc.			
Seguridad general	**SI**	**NO**	**N/S**
25. La empresa donde labora, ¿cuenta con las normas y equipamiento de seguridad de defensa civil?			
26 ¿Cuenta con capacitación periódica sobre medidas de seguridad ante un desastre natural?			
27. Personal de seguridad, ¿Realiza simulacros de evacuación ante un desastre natural?			

Si tiene alguna sugerencia, opinión, o propuesta para mejorar la seguridad en los puntos mostrados de la encuesta, por favor redactarlo en las siguientes líneas de lo contrario agradecemos con su colaboración

_____

_____

_____

_____

Muchas gracias
Michael Salinas Rodríguez
Ing. Electrónico
Julio Valencia Moncada
Ing. De Sistemas