UNIVERSIDAD ALAS PERUANAS

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

"APLICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD INFORMÁTICA AL CENTRO DE DATOS EN LA EMPRESA MIBANCO"

PRESENTADO POR EL BACHILLER

APARCANA FLORES, FIORELLA PATRICIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

ICA – PERÚ
2017

DEDICATORIA

A Dios, por el don de la vida, por una familia maravillosa y por ser guía de cada uno de nuestros pasos.

A mis queridos Padres, y a toda mi familia, por sus consejos, sus valores, por el ejemplo y la motivación constante que me ha permitido ser una persona de bien, pero sobre todo, por amor.

A los docentes por haberme guiado en todo el proceso de elaboración de la Tesis.

AGRADECIMIENTOS

A mis Padres por confiar siempre en mí, apoyándome en todas las decisiones que he tomado en mi vida.

A mis maestros, por sus consejos y por compartir sus amplios conocimientos y experiencia.

A todos los **docentes de la Escuela Profesional de Ingeniería de Sistemas e Informática** por la formación brindada durante mis estudios.

RESUMEN

La presente tesis realiza la evaluación del impacto de la Aplicación de la Política General Informática en la Empresa MiBanco.

El principal problema encontrado, es que la institución financiera no cuenta con un Política General de Seguridad informática, por ende los datos e información almacenada en su centro de datos se encuentra expuesta a amenazas y riesgos físicos, debido a inadecuados procedimientos y políticas de Seguridad. Asimismo se ve con frecuencia el ingreso de virus al sistema, la actualización de parches del sistema se lleva a cabo sin una política establecida, por lo que en algunas ocasiones se genera la caída del sistema lo que ocasiona pérdida de tiempo en la restauración así como en la respuesta a los incidentes que se crean como consecuencia de estas caídas fortuitas del sistema, lo que lógicamente genera también costos adicionales a la empresa.

El método empleado es el método científico, y diseño cuasiexperimental porque se manipula deliberadamente al menos una variable independiente para ver el efecto en las variables dependientes. En relación a las técnicas, se emplearon entrevistas y observación de campo; y respecto a los instrumentos se utilizaron las fichas digitales y guías de entrevista.

La hipótesis general planteada es: Si se aplica la Política General de Seguridad Informática entonces influye positivamente en el Centro de Datos de la Empresa Mibanco de la ciudad de Lima, para lo cual se establecieron 05 indicadores, los cuales en su totalidad, aceptaron la hipótesis alterna la cual resulta a favor de la hipótesis general; lo cual demostró al final de la presente investigación que la aplicación de un documento de esta naturaleza en la empresa MiBanco, daría un gran valor agregado.

Palabras claves: MiBanco, Política General de Seguridad Informática, Auditoría.

ABSTRACT

This thesis makes the assessment of the impact of the application of the General Policy of Information Security in the MiBanco Company.

In order to conduct the investigation had to do quite a theoretical basis that allows all the details of the technology used and the main reason for its use.

In the first chapter of this project we will observe this information with different backgrounds that serve as samples on which we could base some project criteria.
In the next two chapters we have defined our overall work plan, setting the necessary parameters regarding the approaches required for any research project and strategies to implement in order to accomplish this.

On this basis we proceed to carry out the activities that our methodological approach established, obtaining the data required to proceed in the next chapter, the analysis of these in order to make a statistical evaluation of the data and correct interpretation results.

Already in the final chapter we proceeded to perform the testing of the results obtained in the analysis of data against our hypotheses by different statistical and mathematical methods that allowed ensure the reliability of our results.
Then we established our findings and provide some recommendations needed to complement this research.

Keywords: MiBanco, General Policy Information Security, Audit.

INTRODUCCIÓN

Actualmente Mibanco no cuenta con los parámetros mínimos de seguridad ante posibles eventualidades, el trabajo dentro del centro de datos, se lleva de manera informal en muchos de sus procesos, cuentan con una política de procedimientos que no está normado acorde con la realidad existente en la empresa y no garantiza la protección de la información, valor más preciado para una empresa, en tal sentido la presente investigación de tesis pretende reducir el riesgo que esto significa.

Siendo el objetivo principal de la tesis, determinar la medida en que la aplicación de una Política General de Seguridad Informática puede influir de manera positiva en el Centro de Datos de la Empresa.

Para poder realizar la investigación se tuvo que hacer todo un sustento teórico que permita conocer todos los detalles de la tecnología utilizada y el motivo principal de su uso.

En el primer capítulo del presente proyecto podremos observar esta información junto con diferentes antecedentes que sirven de muestras, sobre las cuales hemos podido basar algunos criterios del proyecto.

En los dos siguientes capítulos hemos definido nuestro esquema total de trabajo, estableciendo los parámetros necesarios con respecto a los planteamientos requeridos para todo proyecto de investigación y las estrategias a aplicar para poder llevar a cabo esta.

Con esta base se procede a realizar las actividades que nuestro planteamiento metodológico estableció, obteniendo así los datos requeridos para poder proceder, en el siguiente capítulo, a realizar el análisis de estos con la finalidad de hacer una evaluación estadística de los datos y una correcta interpretación de los resultados.

Ya en el capítulo final se procedió a realizar la contrastación de los resultados obtenidos en el análisis de los datos frente a nuestras hipótesis por medio de diferentes métodos estadísticos y matemáticos que permitieron asegurar la confiabilidad de nuestro resultado. Luego establecimos nuestras conclusiones y brindamos algunas recomendaciones, necesarias para complementar esta investigación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

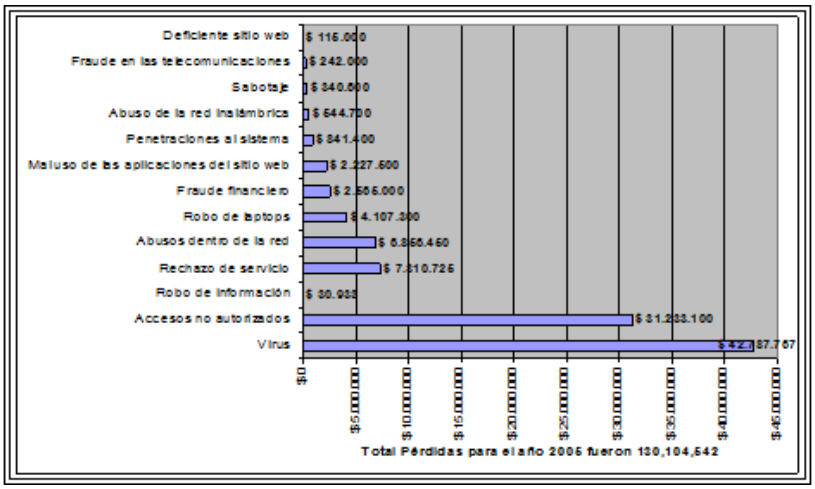
CAPÍTULO I
PLANTEAMIENTO METODOLÓGICO

1.1. Descripción de la Realidad Problemática.

La información es importante para todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablemos de empresas altamente automatizados por lo que su seguridad sigue siendo un punto pendiente en las empresas, basta con mirar sus actividades para darnos cuenta que la seguridad es el factor más determinante por el cual fracasan las organizaciones.

Así nos lo hace notar el estudio CSI/FBI año 2010, realizado por el Instituto de Seguridad en Computación con la participación de la Agencia Federal de San Francisco, escogiendo una muestra de 700 empresas de Estados Unidos, las cuales revelaron sus pérdidas causadas por tipo de amenaza de computadoras. Las pérdidas totales para el año 2010 eran de $130,104,542 para las 700 empresas que respondieron a este estudio, mostrando la gráfica que mayores pérdidas se presentan en los virus, acceso no autorizado y el robo de información en comparación a las demás problemas que presentan las organizaciones. Se sospecha que el aumento en esas tres amenazas podría ser efecto del abuso y uso indiscriminado del internet por parte de los integrantes de la empresa.

Figura 1: Pérdidas por tipo de amenaza

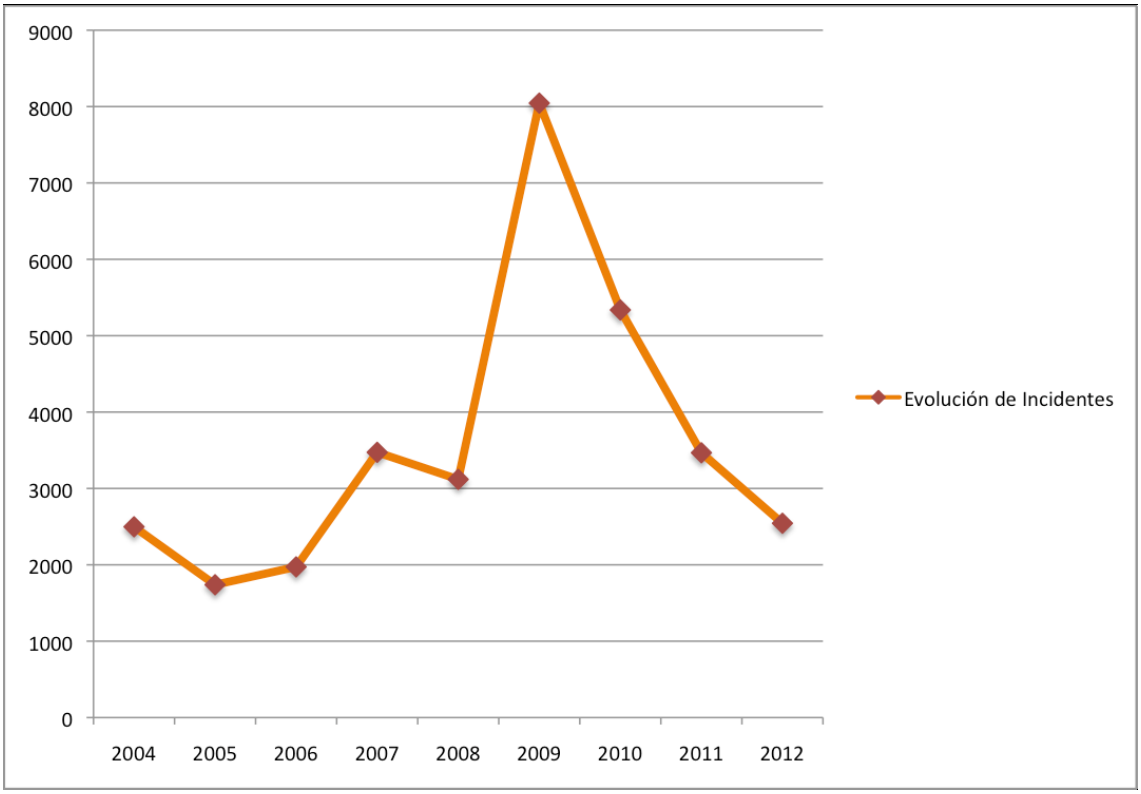


Fuente: CSI/FBI 2010 Computer Crime and Security Survey

Es muy importante ser conscientes de que por más que nuestra empresa a nuestro criterio sea la más segura, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas.

Es así como lo demuestra un estudio realizado por el grupo de seguridad Red IRIS que ha tomado como población a las empresas de España ya que de este país es de donde recibe mayor cantidad de denuncias acerca de incidentes de seguridad cuyo objetivo ha sido el de reflejar el incremento de estos desde el año 2004 hasta el 2012; obteniendo los siguientes resultados:

Figura 2: Tendencia de incidentes de inseguridad



Fuente: http://www.rediris.es/cert/servicios/iriscert/incidentes.html

Las cifras detalladas son las siguientes:

Figura 3: Tendencia de incidentes de inseguridad

Año	Incidentes Totales	Incremento
2004	2682	107.26%
2005	1739	-35.16%
2006	1973	13.45%
2007	3473	76%
2008	3119	-10.19%
2009	8045	157.93%
2010	5337	-33.66%
2011	3469	-35%
2012	2544	-26.6%

Fuente: **http://www.rediris.es/cert/servicios/iriscert/incidentes.html**

Sin embargo, gran parte de esa concientización está en manos de los responsables de seguridad de la información apoyados en todo momento por la gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas, impartiendo así procedimientos de actuación que permitan que las medidas técnicas que se disponen desde informática sean efectivas.

Por lo tanto en este nuevo entorno, es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio, sino también las de sus inversores, clientes, socios y empleados, reduciendo los problemas de seguridad que pueden surgir y dando a la información su valor.

Mibanco no cuenta con los parámetros mínimos de seguridad ante posibles eventualidades, el trabajo dentro del centro de datos, se lleva de manera informal en muchos de sus procesos, cuentan con una política de procedimientos que no está normado acorde con la realidad existente en la empresa y no garantiza la protección de la información, valor más preciado para una empresa, en tal sentido la presente investigación de tesis pretende reducir el riesgo que esto significa.

1.2.1. Delimitaciones.

A. Delimitación Espacial.

El proyecto se realizará en la oficina principal de Mibanco, ubicado en la Av. Domingo Orue 165 - Surquillo.

Mibanco cuenta cinco principales sistemas: el sistema TOPAZ y un sistema ADRYAN, TRADERLIVE, ICS y EBS. La información se obtendrá del Sistema TOPAZ, el cual posee datos relacionados con los gastos que realiza Mibanco en su oficina principal y demás agencias.

B. Delimitación Temporal.

Para el cumplimiento de la investigación, el proceso demanda el desarrollo de dos etapas:

1. Primera etapa, De enero a julio del 2013 después de evaluar referencias bibliográficas como: libros, páginas de internet, etc., se realiza la formulación del problema, los objetivos que tiene nuestra investigación, justificación e importancia del estudio y delimitación del problema.

También se utilizan técnicas de recolección de datos las cuales nos ayudan a ver cómo vamos avanzando en la investigación y cuáles son nuestros resultados, se hallan las Variables e Indicadores, se realiza la Cobertura de Estudio y el Marco Teórico.

2. Segunda etapa, De agosto a diciembre del 2013**.** Aquí se describen, analizan e interpretan los datos y se realiza la discusión de datos obtenidos mediante la aplicación de los instrumentos, en base a las variables e indicadores propuestos, también se realiza la descripción de la construcción de la herramienta.

Finalmente, redactamos las conclusiones, sugerencias, referencias bibliográficas y anexos donde adjuntamos la matriz de consistencia y los instrumentos de medición.

C. Delimitación Social.

En la investigación están involucrados los siguientes roles sociales:

- El Investigador
- El Asesor
- El Gerente de la Empresa
- El personal del área de Sistemas
- Usuarios de los Sistemas de Información

D. Delimitación Conceptual.

Información: Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización. La información da las pruebas de la calidad y circunstancias en las que se encuentra la empresa.

Vulnerabilidad: Cualquier debilidad en los Sistemas que pueda permitir a las amenazas causarles daños y producir pérdidas.

Amenaza: Cualquier evento que pueda provocar daño a la información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa.

Incidente de seguridad: Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza.

Seguridad de Información: Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas

informáticos ante cualquier amenaza, un proceso en el cual participan además personas.

Razones de vulnerabilidades de los Sistemas

Existen muchas ventajas para los sistemas de información que están adecuadamente salvaguardados. Pero cuando grandes cantidades de datos están almacenados electrónicamente, son más vulnerables que cuando se tienen en forma manual.

Estas vulnerabilidades se pueden originar por factores técnicos, institucionales, ambientales y en conjunto por malas decisiones administrativas.

Los sistemas computarizados son especialmente vulnerables a tales desafíos por las siguientes razones:

•Complejidad en los sistemas de información: Un sistema de información complejo no puede ser duplicado a mano. La mayor parte de la información no puede imprimirse o es demasiado voluminosa para ser tratada manualmente.

•Registros propios del computador: En general no quedan huellas visibles de cambios en los sistemas computarizados, porque los registros de computadoras solo pueden ser leídos por la máquina.

•Procedimientos computarizados: Parecen ser invisibles y no son bien entendidos y auditados.

•Por cambios: Los cambios en los sistemas automatizados son más costosos y con frecuencia más complejos que los cambios en los sistemas manuales.

•El desarrollo y operación de los sistemas: Los sistemas están abiertos al abuso de miembros del personal altamente capacitados técnicamente que no estén bien integrados a la institución. (Los programadores y los

operadores de computadoras pueden hacer cambios no autorizados en el software mientras la información se procesa o pueden utilizar instalaciones de cómputo para propósitos no autorizados. Los empleados pueden hacer copias no autorizadas de archivos de datos con fines ilegales.)

•Sistemas automatizados: Aunque las posibilidades de desastre en los sistemas automatizados no son mayores que en los sistemas manuales, el efecto puede ser mucho mayor. En algunos casos, todos los registros del sistema pueden quedar destruidos y perdidos para siempre.

Se tienen menos documentos en papel para procesar y revisar cuando los sistemas están automatizados. Es posible tener menor inspección manual.

•Acceso a los sistemas: La mayor parte de los sistemas son accesibles a muchas personas. La información es más fácil de recopilar pero más difícil de controlar.

•Procesamiento de datos: Los datos en los sistemas de cómputo pasan por más pasos de procesamiento que en los sistemas manuales, cada uno de los cuales está abierto a errores o a abusos. Cada una de estas funciones (origen de los datos, registro, transmisión, procesamiento, almacenamiento, recuperación y distribución) requiere de un conjunto independiente de controles físicos, administrativos y técnicos.(2)

Vulnerabilidades

Los avances en las telecomunicaciones y en el software de las computadoras han aumentado las vulnerabilidades a la seguridad de los sistemas que pueden ser interconectados en diferentes puntos, es decir que el potencial para acceso no autorizado, abuso o fraude no se limita a un solo lugar sino que puede ocurrir en cualquier punto de acceso a la red, lo que crea nuevas áreas y oportunidades para penetración y manipulación de los sistemas.

El entorno de internet es un peligro constante para las organizaciones que ahora trabajan con este servicio. Los peligros más frecuentes de los que deben protegerse las empresas mientras navegan en internet sus integrantes son los siguientes:

•Hackers: También llamados piratas informáticos accedan a la información que existe y se transmite por internet, no solo tienen acceso a e-mails sino a computadoras que están enlazadas a la red perjudicando a las empresas haciendo mal uso de la información.

•Cracker: Son personas que intentan romper la seguridad de un sistema, accediendo con malas intenciones a la información que se mantiene guardada en ellos.

•Virus: Son programas diseñados para modificar o destruir datos, pueden ser ingresados al sistema por un dispositivo externo o través de la red (e-mails) sin intervención directa del atacante.

•Gusanos: Son virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

•Caballos de Troya: Son virus que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

•Spam: También llamado correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y organismos.

Pero no sólo el internet es una amenaza para las organizaciones podemos encontrar otras tantas dentro de la propia empresa. Una

amenaza siempre latente es el personal de la organización que por muchas circunstancias puede ser un peligro ya sea por los errores que pueda cometer sin intención como aquellos que son hechos con el objetivo de dañar a la organización un ejemplo claro es cuando en el Departamento de Sistemas no genera registros de las actividades de los usuarios en la red, esto provoca que no se pueda identificar anomalías que pueden realizar los empleados mientras se encuentren conectados al sistema volviendo a la información que se genera poco confiable; si continuamos explorando dentro de la empresa podemos encontrar otras vulnerabilidades como son los equipos que no reciben el mantenimiento adecuado o que por fallas eléctricas suelen dañarse y dejar a la organización con menos recursos para realizar sus operaciones. Las organizaciones siempre estarán expuestas a estos tipos de riesgos o ataques informáticos y a otros más ya que a medida que avanza la tecnología también habrá personas que intenten mejorar las formas de vulnerar la seguridad.

1.2.2. Definición del Problema.

Continuamente, las personas deben elegir de entre varias opciones aquella que considera más conveniente. Es decir, han de tomar gran cantidad de decisiones en su vida cotidiana, en mayor o menor grado importantes, a la vez que fáciles o difíciles de adoptar en función de las consecuencias o resultados derivados de cada una de ellas.

Es posible trasladar este planteamiento general al ámbito de la División de Soporte Centralizado de Mibanco; ya que no se escapa de esta realidad. La toma de decisiones abarca a las cuatros funciones administrativas, así los administradores cuando planean, organizan, conducen y controlan, se les denomina con frecuencia los que toman las decisiones.

Como tomar una decisión supone escoger la mejor alternativa de entre las posibles, se necesita información sobre cada una de estas alternativas y sus consecuencias respecto a nuestro objetivo. La importancia de la información en la toma de decisiones, entendiendo por esta "el proceso de transformación de la información en acción". La información es la materia prima, el input de la decisión, y una vez tratada

adecuadamente dentro del proceso de la toma de decisión se obtiene como output la acción a ejecutar.

La realización de la acción elegida genera nueva información que se integrará a la información existente para servir de base a una nueva decisión origen de una nueva acción y así sucesivamente. Y servirá como Feed-back.

De esta manera en el proceso de la toma de decisiones de Mibanco, para la división de Contraloría y Finanzas, necesita de la información necesaria en base a los objetivos trazados que tiene como división, en la cual existe este problema debido a que no se cuenta con la información necesaria a tiempo para poder generar o tomar acciones para luego evaluar el impacto de los resultados, además de capturar esa información como base para una nueva decisión.

Actualmente Mibanco no cuenta con un Política General de Seguridad de la Información informática, por ende los datos e información almacenada en su centro de datos se encuentra expuesta a amenazas y riesgos físicos, debido a inadecuados procedimientos y políticas de Seguridad, se ve con frecuencia el ingreso de virus al sistema lo que ocasiona que constantemente se esté alerta con esta amenaza y se tiene que están constantemente eliminando dichos virus, de la misma forma se tiene que estar actualizando los parches del sistema sin una política establecida, por lo que en algunas ocasiones se genera la caída del sistema y se tiene que ocupar tiempo en restaurarlo, ocasionando pérdida de tiempo, de la misma manera se pierde tiempo en la respuesta a los incidentes que se crean como consecuencia de las caídas fortuitas del sistema ocasionando costos adicionales a la empresa.

1.3. Formulación del Problema.

¿En qué medida la aplicación de la Política General de Seguridad Informática influye en el Centro de Datos de la Empresa Mibanco de la ciudad de Lima?

1.4. Objetivo de la Investigación.

Determinar la medida en que la aplicación de la Política General de Seguridad Informática influye en el Centro de Datos de la Empresa Mibanco de la ciudad de Lima.

1.5. Hipótesis de la Investigación.

Si se aplica la Política General de Seguridad Informática entonces influye positivamente en el Centro de Datos de la Empresa Mibanco de la ciudad de Lima.

1.6. Variables e Indicadores.

1.6.1. Variable Independiente.

X1= Aplicacion de la Política General de Seguridad Informática

Operacionalización de Indicadores.

Tabla 1 : Indicadores de la Variable Independiente

Indicador	U. de Medida	Índice	U. de Observación
X1= Aplicación de la Política General de Seguridad Informática	-.-	NO / SI	Análisis Documental

A. Conceptualización de Indicadores.

Tabla 2: Conceptualización de la Variable Independiente

Indicador	Conceptualización
X1= Aplicación de la Política General de Seguridad Informática	La política del sistema en la empresa.

1.6.2. Variable Dependiente.

Y1= Centro de Datos

A. Operacionalización de los Indicadores.

Tabla 3: Indicadores de la Variable Dependiente

Indicador	U. de Medida	Índice	U. de Observación
Y1= Porcentaje de Virus detectados y eliminados oportunamente (VDE)	-	[300…600]	Observación
Y2= Cantidad de parches críticos aplicados (CPA)	-	[180..420]	Observación
Y3= Tiempo de restauración de un sistema (TRI).	Minutos	[600..1200]	Observación
Y4= Tiempo de respuesta para un incidente	Minutos	[60..180]	Observación
Y5= Costo que demanda solucionar un incidente	Soles	[480..900]	Observación

B. Conceptualización de los Indicadores.

Tabla 4: Conceptualización de la Variable Dependiente

Indicador	Conceptualización
Y1= Porcentaje de Virus detectados y eliminados oportunamente (VDE)	Porcentaje de virus que se detectaran y eliminaran de manera oportuna y efectiva.
Y2= Cantidad de parches críticos aplicados (CPA)	Cantidad de parches a las aplicaciones y los sistemas funcionen adecuadamente sin paralizaciones ni errores,
Y3= Tiempo de restauración de un sistema (TRI).	Tiempo que se toma para restaurar un sistema en Mi Banco
Y4= Tiempo de respuesta para un incidente	Tiempo que se emplea para generar la respuesta a un incidente
Y5= Costo que demanda solucionar un incidente	Costo que se toma para solucionar un incidente.

1.7. Viabilidad de la Investigación.

1.7.1. Viabilidad Técnica.

Técnicamente ha sido viable la investigación debido a que se cuenta con la tecnología necesaria para la implementación del Política General de Seguridad Informática.

1.7.2. Viabilidad Operativa.

La investigación ha sido operativamente viable toda vez que la entidad Financiera Mi banco ha tenido la predisposición a la aplicación del Política General de Seguridad Informática.

1.7.3. Viabilidad Económica.

El trabajo de investigación es económicamente viable ya que el costo incurrido en las distintas etapas del estudio de investigación será cubierto por el investigador.

1.8. Justificación e Importancia de la Investigación.

1.8.1. Justificación de la Investigación.

Se justifica la investigación, ya con su aplicación se va a beneficiar a la institución ya que se reducirá la infección de los archivos con motivo de virus, los ataque a la institución de la misma manera serán reducidos por la seguridad implementada, se aumentará la instalación de parches a las aplicaciones y los sistemas funcionen adecuadamente sin paralizaciones ni errores, se reducirá el tiempo en restaurar la falla en los sistemas de información, y con ello finalmente se reducirá el costo de atención a los incidentes presentados.

1.8.2. Importancia de la Investigación.

La investigación es importante debido a que su aplicación tendrá un gran impacto en la empresa, ya que los sistemas de información tendrán un mejor desempeño al evitar las paralizaciones de los sistemas, no interrumpiendo las actividades de atención a los clientes y los usuarios de los sistemas de la empresa.

1.9. Limitaciones de la Investigación.

El proyecto se realizará en la oficina principal de Mibanco, ubicado en la Av. Domingo Orue 165 - Surquillo.

La información se obtendrá del Sistema TOPAZ, el cual posee datos relacionados con los gastos que realiza Mibanco en su oficina principal y demás agencias.

La elaboración del mapa estratégico estará basada en los objetivos, la misión y la visión de la división de Contraloría y Finanzas y las relaciones con las distintas perspectivas del Cuadro de Mando Integral.

1.10. Tipo y Nivel de la Investigación.

1.10.1. Tipo de Investigación.

La naturaleza de la investigación es **Aplicada,** porque busca el conocer para hacer, para actuar, para construir, para modificar. [1]

Porque su propósito fundamental es dar solución a problemas y se da como un conjunto de actividades destinadas a utilizar resultados de las ciencias y tecnologías. [2]

1.10.2. Nivel de Investigación.

La investigación empezó con un nivel **Descriptivo**, porque busca desarrollar una imagen o fiel representación (descripción) del fenómeno estudiado a partir de sus características. Describir en este caso es sinónimo de medir. Miden variables o conceptos con el fin de especificar las propiedades importantes de comunidades, personas, grupos o fenómenos bajo análisis. El énfasis está en el estudio independiente de cada característica, es posible que de alguna manera se integren las mediciones de dos o más características con el fin de determinar cómo es o cómo se manifiesta el fenómeno.

---

[1] G., Tevni Grajales. [En línea] http://tgrajales.net/investipos.pdf.

[2] John, Hayman. *investigación y solución* . Buenos Aires : Editorial Paidos, 1969.

El trabajo finaliza con un nivel **Correlacional**, porque pretenden medir el grado de relación y la manera cómo interactúan dos o más variables entre sí. Estas relaciones se establecen dentro de un mismo contexto, y a partir de los mismos sujetos en la mayoría de los casos.[3]

1.11. Método y Diseño de la Investigación.

1.11.1. Método de la Investigación.

Para el desarrollo de esta tesis se ha utilizado el **método científico**, porque proporciona un planteamiento ordenado y un nivel de rigurosidad alto en el tratamiento de los datos y análisis de resultados.[4]

1.11.2. Diseño de la Investigación.

Para el desarrollo de esta tesis se ha utilizado el **diseño cuasiexperimental**, porque manipulan deliberadamente al menos una variable independiente para ver su efecto y relación con una o más variables dependientes. [5]

$$Ge : O_1 \; X \; O_2$$

Dónde:

Ge= Grupo experimental.

O1= Observación inicial (Preprueba).

X = Tratamiento experimental

O2 = Observación final (Postprueba).

1.12. Técnicas e Instrumentos de Recolección de Información.

1.12.1. Técnicas.

Las principales Técnicas que se han utilizado para el levantamiento de información son:

- Entrevistas
- Observación de Campo

[3] G., Tevni Grajales. [En línea] http//es.crebd.com/doc/15246394/Tipos y Niveles Investigación 2009.

[4] Sabino, Deza Jaime y Muñoz. *Metodología de la Investigación Científica.* Perú : Ediciones Universidad Alas Peruanas, 2008. p.13.

[5] Hernandez Sampieri, Roberto. Metodología de la Investigación. 4ta Edición. México. 2006. Mc Graw Hill. pp.

1.12.2. Instrumentos.

Los Instrumentos utilizados fueron los siguientes:

- Fichas Digitales
- Guía de entrevista

1.13. Cobertura de Estudio.

1.13.1. Universo

Teniendo en cuenta el horizonte de la investigación, el universo está conformado por todos los resultados obtenidos de la aplicación de la Política General de Seguridad de la Información que demandan los servicios que brinda la MiBanco en la ciudad de Lima.

1.13.2. Población

La población está compuesta por los resultados obtenidos de la aplicación de la Política General de Seguridad de la Información, para el desarrollo de la presente investigación en la empresa MiBanco comprendido en el periodo del 3 de agosto al 31 de diciembre del 2013.

1.13.3. Muestra

La muestra será efectuada por la siguiente fórmula:

Datos:

$$n = \frac{N\, Z^2_{1-\frac{\propto}{2}}\, S^2}{d^2(N-1) + Z^2_{1-\frac{\propto}{2}} S^2}$$

e = Error Permisible de 5%

$Z^2_{1-\alpha/2}$ = Medida de Estimación, significancia al 95%: 1.96

S = Desviación estándar de: 26%

La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la Investigación.

Se revisaron las fuentes de información bibliográficas, tanto primarias, como secundarias y terciarias a efectos de investigar la existencia de trabajos previos similares al presente; sin embargo, no se ha encontrado publicación alguna al respecto, razón por la cual, se puede afirmar que este trabajo de investigación, como contenido y como enfoque es inédito. Sin embargo, existen investigaciones realizadas bajo otro contexto como es el caso de:

1. **Tesis: Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú. Universidad Pontificia Universidad Católica del Perú (2014)**
   Autor: Aguirre Mollehuanca, David Arturo.
   Pais: **Lima – Perú**

Resumen

La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo. En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización así como identificar y evaluar los riesgos a los cuales estos estaban sometidos. Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles

de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

2. Tesis: Gestión de seguridad de la información y los servicios críticos de las universidades – Universidad Nacional Mayor de San Marcos (2007)

Autor: Ruben Alejandro, Rayme Serrano

Pais: Lima - Perú

Resumen:

Existe una actitud histórica en la educación superior según la cual no debe haber restricciones para el acceso a la información; es en ese sentido que los docentes, alumnos, investigadores y terceros solicitan el acceso abierto a los sistemas de información de las Universidades. Sin embargo a la luz de las recientes amenazas de la información tales como: sabotajes, violación de la privacidad, intrusos, interrupción de servicios, etc. y de las expectativas de mayores amenazas a la seguridad en el futuro, no puede continuar este acceso abierto e ilimitado. Por esta razón se realizó un estudio en tres Universidades de Lima Metropolitana: la Universidad Nacional Mayor de San Marcos (UNMSM), la Universidad Nacional Federico Villarreal (UNFV) y la Universidad Privada San Juan Bautista (UPSJB), teniendo como objetivo proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las universidades. Cabe señalar que la muestra de la población estuvo conformada por 30 expertos del área de Tecnología de Información y Comunicaciones (TIC) que laboran en las 3 universidades citadas, a quienes se les aplicó un formulario de encuesta para medir sus opiniones con respecto a la gestión de seguridad y los servicios críticos. Los resultados de la investigación revelaron las estrategias que se deben utilizar en la gestión de seguridad de la información como son: primero, la importancia de desarrollar políticas de seguridad: UNMSM 37 %, UNFV 19% y UPSJB 24%; segundo, los programas de capacitación al personal, donde los expertos consultados informaron el interés por asistir : UNMSM 60%, UNFV 70% y UPSJB 70% y tercero, la protección a los recursos de información, porque el 38% de los expertos manifestaron que sus centros informáticos no poseen equipos de protección contra cortes de energía eléctrica, amenaza que

fue común en la década de 1980 -1990. Los resultados también demostraron que al implementarse estas estrategias el impacto en las aplicaciones de red e internet será eficaz y de acuerdo a los expertos consultados se obtendrán beneficios tales como: una mejor protección de la información (50%) y una mejora de la calidad en el servicio a los alumnos y docentes (27%). Además se minimizarán los riesgos de la información, pues en el caso de la UNMSM la infección de virus informáticos es de 56%, mayor al de las otras universidades consultadas. Con respecto a las incidencias de seguridad como son: la modificación desautorizada, divulgación ilícita y robo de la información, los resultados corroboraron lo que está pasando a nivel mundial donde el 70% de ellas son causados por los trabajadores, producto de errores, descuidos en sus conocimientos sobre la seguridad o por actos delictivos propiamente dichos. Por otro lado, debemos recomendar a las autoridades universitarias desarrollar políticas de seguridad de la información o si las tienen hacerlas cumplir porque constituyen la base de un plan de seguridad. De la misma forma, es conveniente un programa educativo de toma de conciencia de seguridad relacionado con la capacitación de los trabajadores. También es necesario reestructurar las redes informáticas aplicando tecnología de prevención y detección de intrusos y separando el área académica con la administrativa pues ambos poseen servicios críticos. Finalmente, se recomienda una propuesta piloto de un plan de seguridad de la información para las Universidades, que servirá para que éstas puedan tomarla como referencia para la implantación de sus propios planes de seguridad

3. **Tesis: Diseño e Implementación de un Sistema de Gestión de la Seguridad de la Información en Procesos Tecnológicos - Universidad San Martín de Porres (2012)**
   Autor: Carlos Eduardo, Barrantes Porras; Javier Hugo Herrera.
   Pais: Lima – Perú

   Resumen:
   En la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia esta corre riesgos al igual que sus activos. El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de

la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005. Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad. La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una empresa; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos. La problemática principal actual de las empresas que desean incursionar en el ámbito financiero es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a pérdidas no solo de información, sino también económica. Es por ello, que Card Perú S.A. se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

2.2. Marco Histórico

2.2.1 Política General de Seguridad Informática

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como:

- **Crítica**: Es indispensable para la operación de la empresa.
- **Valiosa**: Es un activo de la empresa y muy valioso.
- **Sensible**: Debe ser conocida por las personas autorizadas Los términos de seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

La información es la base fundamental sobre la cual la seguridad desarrolla su dinámica y propone las acciones de protección. En este sentido, las motivaciones de control y confiabilidad han venido evolucionado con el paso de los años. En los años 70 con el nacimiento de los sistemas de computación o mainframes, donde se contaban con máquinas de procesamiento de datos centralizados, las características de seguridad se concentraban en controles propios y particulares al hardware y software de los proveedor de dichas tecnologías. En este contexto, firmas como IBM y WANG, daban los lineamientos generales de seguridad y control ajustados a sus equipos, indicando aspectos técnicos de operación, seguridad física, recuperación ante desastres, así como la segregación funcional necesaria para mantener controlada y confiable la operación del sistema. Con el pasar de los años, en los 80 con el surgimiento de las

redes de computadores y un animado flujo de información entre diferentes puntos, las motivaciones de seguridad de la información salen de la máquina central, a un conjunto o colección de máquinas, las cuales generan nuevos retos para los encargados de las tecnologías de información como son entre otros las fallas de la suite de protocolos TCP/IP, las exigencias de las aplicaciones en el entorno cliente/ servidor, la administración remota de máquinas, la administración de la infraestructura de seguridad de la información. Ya para los años 90 con una alta penetración del uso de Internet, con una fuerte demanda de servicios en el web y con un individuo exigente por innovación y productos informáticos en la red, los encargados de TI advierten nuevas motivaciones alrededor del tema de seguridad de la información. Por tanto, con una alta exposición del usuario final a las herramientas y servicios en la red, y un desmedido deseo de explorar y conocer, basado en la aparente confianza que le brinda Internet, la información circula con mayor libertad y las infraestructuras empresariales requieren mayores canales de comunicación y estrategias de protección que antes no eran pensables. Los gusanos, el software espía, los código maliciosos móviles, la suplantación de identidad, entre otros elementos conforman el escenario de plagas informáticas que deben ser atendidas por los especialista en TI. En lo corrido de la primera década de este nuevo milenio, se advierte un nuevo cambio de foco en la seguridad de la información.

La tarea de establecer y mantener las políticas de seguridad de información corresponde al administrador de seguridad de información, quien debe implementar procesos para lograr ello. La institución financiera debe asegurar que estas políticas sean parte integral de su administración. Se deben considerar como “documentos vivientes” que deben ser revisados con regularidad para asegurar se mantengan actualizados ante cualquier cambio (tecnológico, organizacional, de procesos, etc.) en la institución financiera. Se debe formalizar la periodicidad de revisión de las políticas y los criterios para dicha revisión. A partir de acá, los estándares se revisan y modifican para direccionar los cambios en las políticas. Los procedimientos y

guías se derivan de las políticas de seguridad. Las políticas de seguridad de información sirven a varios propósitos, estableciendo primariamente lo que está o no permitido. Además éstas deben alinearse apropiadamente a los objetivos de negocio. Algunos métodos para lograr este último propósito se citan a continuación:

- Determinar si las inversiones en seguridad de información son proporcionales o no con el perfil de riesgo de la institución y los objetivos de negocios.
- Determinar la clasificación de la información requerida para la institución, con la finalidad de implementar las políticas necesarias. Determinar si las políticas de seguridad han sido adecuadamente diseñadas, implementadas y reforzadas para proteger la información de la institución.

Los enunciados de las políticas deben ser lo suficientemente genéricos de manera que no sea necesario cambiarlos con mucha frecuencia; ni se presten a interpretaciones ambiguas. No es apropiado tener políticas que sean tan específicas que tengan que ser reformuladas cada vez que cambia la tecnología.

2.2.2 Centro de Datos

Se denomina centro de datos a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Iberoamérica, o centro de cálculo en España o centro de datos por su equivalente en inglés data center. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

Una data center te ofrece varios niveles de resistencia, en la forma de fuentes de energía de Backup y conexiones adicionales de comunicación, que puede no ser utilizada hasta que pase algún problema en el sistema primario donde el principal objetivo de un proyecto de data center es ejecutar las aplicaciones centrales del negocio y almacenar datos operativos, donde ofrece las aplicaciones más tradicionales que es el sistema de software corporativo como

Enterprise Resource Planning (ERP) y Customer Relationship Management (CRM). Los componentes más comunes son firewalls, gateways VPN, routers y computadores, servidores de banco de datos, de archivos aplicaciones, web y middleware, todo en hardware físico o en plataformas consolidadas y virtuales izadas. Data center es utilizada internacionalmente para medir la eficiencia de los términos de energía que es ofrecida para todas las instalaciones comparada a la energía usada por equipos de TIC, y ofrece una taza de eficiencia, el equipo TIC puede consumir 800Kw, y los sistemas de enfriamiento consumen otros 800Kw.

2.3. Marco Conceptual

2.3.1 Seguridad Informática

La seguridad informática, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.1 Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad informática es la disciplina que se ocupa de

diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

2.3.2 Importancia de la Seguridad de la Información.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

En nuestro medio no existe una conciencia acerca de la importancia de la seguridad informática, debida a que las organizaciones se concentran en su core business y piensan que nunca van a ser atacadas o vulneradas en sus sistemas informáticos. Por esta misma razón no le asignan al tema de la seguridad informática la importancia que merece hasta que se presenta una eventualidad que hace reconsiderar ese aspecto pero a unos costos altísimos por efectos de la penetración. Cuando se presenta un ataque, la crisis pone a cualquier compañía en desventaja frente a sus competidores, incluso, puede causar su quiebra si no responde con rapidez a las exigencias del mercado. Por ello, es vital para toda organización el aseguramiento de su información, proceso que debe ser acompañado permanentemente para conseguir resultados confiables. Cabe destacar que la seguridad de los sistemas, por mayores soluciones que se implementen, nunca será del 100 por ciento; por ello aunque una compañía ya cuente con un sistema de seguridad informática, es necesario que sea probado o auditado por un tercero, para descubrir sus niveles de vulnerabilidad, que entre otros, puede originarse al interior de la compañía.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
- La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

2.3.3. Control Interno Informático

El Control Interno Informático es una función del departamento de Informática de una organización, cuyo objetivo es el de controlar que todas las actividades relacionadas a los sistemas de información automatizados se realicen cumpliendo las normas, estándares, procedimientos y disposiciones legales establecidas interna y externamente.

El Control Interno Informático se puede definir como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados. El control interno no tiene el mismo significado para las personas, esto puede dificultar su comprensión dentro de una organización. Es un proceso llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de

seguridad "razonable" para la consecución de sus objetivos. Una segunda definición definiría al control interno como “el sistema conformado por un conjunto de procedimientos (reglamentaciones y 23 actividades) que interrelacionadas entre sí, tienen por objetivo proteger los activos de la organización.

2.3.4. SYMANTEC MESSAGING GATEWAY

Permite a las organizaciones proteger su infraestructura de correo electrónico y productividad con protección en tiempo real contra software malicioso y spam, y ataques dirigidos. Dispone de filtrado de contenidos avanzado, prevención contra la pérdida de datos y cifrado del correo electrónico eficaz y preciso. Messaging Gateway es una solución sencilla de administrar que captura más del 99% del spam con menos de un falso positivo en un millón. Proteja el perímetro de su correo electrónico y actúe rápidamente ante las nuevas amenazas de la mensajería con la solución líder del mercado en seguridad de la mensajería.

2.3.5. SYMANTEC ENDPOINT PROTECTION

El aumento de los ataques dirigidos y las amenazas persistentes avanzadas requiere protección en capas y seguridad inteligente en el endpoint. Symantec Endpoint Protection 12.1 ofrece una seguridad inmejorable, un rendimiento deslumbrante y una administración más inteligente en entornos físicos y virtuales. Mediante la red de inteligencia contra amenazas más grande del mundo, Symantec puede identificar archivos en riesgo y detener las amenazas de día cero sin lentificar el rendimiento. Solo Symantec Endpoint Protection 12.1 brinda la seguridad que necesita mediante un único agente sumamente eficaz para la protección más efectiva y rápida disponible.

2.3.6. ORACLE DATA MASKING

- Presentar de manera completa el ciclo de enmascaramiento y creación de subconjuntos de datos en Oracle Enterprise manager 12c.
- Mostrar cómo se crea un modelo de datos y se clasifican datos sensibles.

CAPÍTULO III
CONSTRUCCIÓN DE LA HERRAMIENTA

3.1 Generalidades

Esta propuesta de Política General de Seguridad Informática, la hemos elaborado, con el fin de relevar la consistencia de los sistemas de información y de control, la eficiencia y efectividad de los programas y operaciones, y el cumplimiento de los reglamentos y normas prescritas. Como resultado se detallan las debilidades encontradas y se emiten recomendaciones que contribuyan a mejorar su nivel de seguridad. Esto se llevó a cabo como medio para el desarrollo de un Política General de Seguridad Informática, donde se definen los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad con el objetivo de establecer una cultura de la seguridad en la organización. Asimismo, la obliga a redactar sus propios procedimientos de seguridad, los cuales deben estar enmarcados por las políticas que conforman este plan. El propósito de establecer este plan es proteger la información y los activos de la empresa, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados de la organización.

3.2 Análisis de la Auditoría de Sistemas

3.2.1 Metodología Aplicada

La metodología utilizada para la realización de la presente Auditoría se basa en el desarrollo de las siguientes actividades:

a. Definición de los objetivos de la auditoría.

El objetivo general consiste en la realización de una **Auditoría Informática** con el fin de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una **Política de Seguridad**, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

b. Análisis de fuentes de datos y recopilación de información.

c. Generación del plan de trabajo, asignación de recursos y establecimiento de plazos de tiempo.

d. Generación de cuestionarios y adaptaciones realizadas a los mismos en base a los perfiles de los entrevistados.

e. Proceso de Relevamiento:

f. Desarrollo de un análisis de riesgos.

g. Análisis de los datos relevados, hallazgos de debilidades y generación de recomendaciones.

h. Discusión de resultados y obtención de la conclusión.

i. Planteamiento de políticas de seguridad.

j. Presentación del informe definitivo a las autoridades de La Empresa.

3.2.2 Normativas Empleadas

Se tomaron como referentes las siguientes Normas y Estándares:
-NTP-ISO/IEC 17799: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
-Norma ISO 27001.
-COBIT 5(Control Objectives for Information Technology).
-ITIL 3.0 (Biblioteca de Infraestructura de Tecnologías de Información)

3.2.3 Informe de Relevamiento

La **Auditoría de Sistemas** propuesta comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

A. Evaluación de la Seguridad Lógica

1. Identificación de usuarios

Altas.- Cuando un usuario nuevo ingresa a la empresa, el área de Recursos Humanos toma sus datos, dando de alta su usuario sin embargo, no existe un procedimiento formal a seguir para realizar estas tareas. Si este usuario necesita del sistema informático,

Recursos Humanos hace el pedido al Área de Sistemas, donde se genera el alta del usuario al sistema. Los datos que se ingresan en la cuenta son los siguientes:

- ✓ ID de usuario, inicialmente será el número de legajo, aunque pudimos comprobar que no corresponde realmente con éste número.
- ✓ Password, inicialmente será el número de usuario, y se instruye al usuario para que lo modifique.
- ✓ Nombre y apellido completo, se obtiene del archivo de Recursos Humanos.
- ✓ Fecha de expiración del password de un año. Aunque para algunos usuarios este campo no se completa, permitiendo que nunca se actualice la contraseña.
- ✓ Fecha de anulación de la cuenta para dar de baja la cuenta.

Mantenimiento.- No se lleva a cabo ninguna **revisión periódica ni control** sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

Permisos.- El control de acceso en la empresa no se basa en los **perfiles de los usuarios** y la asignación o denegación de permisos a los mismos, sino más bien en perfiles de grupos.

Inactividad.- Si el usuario permanece un período de tiempo logeado **sin actividad**, el sistema no ejecuta ninguna acción; los administradores solo advierten a los usuarios sobre la necesidad de no dejar las máquinas logeadas e inactivas.

Cuentas de Usuario.- Los usuarios del Área Comercial **no son identificados en forma personal**, sino que usan todos los mismos nombres y contraseña para ingresar al sistema informático. Este módulo del sistema solo permite hacer consultas a las bases de datos, (listas de precios, planes de ventas, etc.) generalmente desde el salón de ventas, pero no les está permitido hacer ninguna modificación a los datos.

No se eliminan los usuarios que vienen por default en el sistema operativo, estas cuentas permanecen activas en el sistema sin que ningún usuario las utilice.

2. Autenticación de usuarios

Cuando un usuario ingresa su password al sistema, aparecen **asteriscos** en lugar de mostrar el dato que está siendo ingresado. Una vez que algún usuario ha logrado logearse en el sistema, **aparece en pantalla el nombre del usuario** logeado.

3. Passwords

Los **passwords** que existen en la empresa son generados en forma manual, sin procedimientos automáticos de generación. Como restricción, deben tener una longitud máxima de 10 caracteres, numéricos o alfanuméricos. Cuando se da de alta un empleado en el sistema, su **password se inicializa** con el mismo nombre de la cuenta (que es igual al número de legajo del usuario), advirtiéndole al usuario que lo cambie, pero sin realizar ningún control sobre la modificación del mismo.

B. Evaluación de la Seguridad en las Comunicaciones

- **UTP en conexiones internas**: la totalidad del tendido de cables en el interior de la empresa se realizó con UTP categoría 5.
- **Switches**: Los switches han sido programados para realizar un tipo de ruteo: direccionan los paquetes transmitidos por sector, según la dirección IP que traen, distinguiendo a que sector de la empresa van. De esta manera, al no repetir los paquetes de datos a toda la red, se disminuye el uso de ancho de banda y se evita la divulgación de los mensajes, mejorando la seguridad de la topología de Bus.
- **Mail:** No todos los empleados tienen una cuenta de mail ya que hay muchos empleados que no necesitan este servicio. Todos los Jefes de Área disponen de una, por este motivo esta vía de comunicación llega a todo el personal de la empresa. Este medio se utiliza para enviar todo tipo de información.

C. Evaluación de la Seguridad de las Aplicaciones

1. Software

En la Empresa hay un servidor, con **sistema operativo** Windows Server 2003 para el servidor de aplicaciones. Como resultado de una auditoría se eligió este sistema operativo por las siguientes razones:

- ✓ Por la confiabilidad.
- ✓ Por el buen control de acceso y la buena generación de logs de auditoría.

2. Seguridad de bases de datos

En la empresa se utiliza el Sql Server para el desarrollo y la administración de los datos. Existe un control que restringe el acceso a ciertos datos críticos en las aplicaciones propias de la empresa, pero no hay una **clasificación formal de estos datos**. No se realizan **controles de acceso lógico**, a las carpetas donde se almacenen los archivos indexados, ya que estos archivos están en una carpeta del servidor no compartida para el resto de la red, a lo que se agregan los controles de seguridad física del servidor

D. Evaluación de la Administración del Centro de Datos

Administración del Centro de Datos

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de sistemas, que es el administrador del centro de datos. Él es el que planifica y delega las tareas a los empleados del centro de datos, generalmente una vez por semana haciendo responsable a cada uno de sus propios tiempos. El administrador es el encargado de reportar al gerente sobre las actividades en el centro de dato. Estos reportes generalmente se realizan a modo de auto evaluación ya que no son un pedido de ningún directivo.

Planes de Sistemas

No se han desarrollado **planes formales** del departamento de sistemas, solo se hace una distribución de tareas semanalmente entre el personal de esta área.

La reingeniería del sistema es el **proyecto** prioritario, luego tienen proyectos a futuro, como es la migración del sistema de archivos a una base de datos. Se van asignando prioridades a las tareas a medida que surgen. No hay normas, estándares o procedimientos en las que se basen para la planificación, el control y la evaluación de las actividades del área de sistemas de información.

Permisos de los Encargados del Centro de Cómputos

Cuando entra un nuevo empleado al centro de datos, no se le asignan los mismos permisos que al resto de los empleados. A modo de ejemplo: no se le otorgan permisos de acceso a Internet ni cuenta de mail mientras están capacitándose en el uso de la herramienta de desarrollo. A medida que le son asignadas más responsabilidades y sean necesarios más permisos, se va modificando su cuenta de usuario. Estos permisos son asignados por el administrador del centro de datos.

Importancia de la Seguridad

Los empleados de la gerencia y de los cargos más altos tienen plena conciencia de la importancia de la seguridad en la empresa, porque fueron ellos los que encargaron el sistema con los requerimientos que tiene actualmente, aunque pudimos comprobar que no siempre cumplen las disposiciones de seguridad impuestas. Los demás empleados de la empresa tienen conocimientos de las normas pero no son conscientes de su importancia.

E. Evaluación del Plan de Contingencias

1. Plan de administración de incidentes

En la empresa no hay **planes formales** para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos. Pero se dispone de backups de hardware y de servicios que prestan terceros para garantizar la continuidad de los servicios ante alguna contingencia. Estos terceros son una aseguradora y personal técnico especializado de mantenimiento externo. Actualmente las emergencias son administradas por el encargado del centro de cómputos aunque no hay **responsabilidades formales** asignadas a los empleados.

2. Backup de equipamiento

Equipamiento de Red

No hay **backup de hardware** debido a que esta red se encuentra asegurada, de manera tal que ante una contingencia física en algún equipo, la aseguradora garantiza la reparación o el reemplazo del dispositivo. Se optó por esta alternativa basándose en un análisis costo / beneficio que abarcó la totalidad de la infraestructura de la empresa, teniendo en cuenta los costos de implementación, mantenimiento, entrenamiento técnico del personal, y de restauración en caso de una emergencia.

3. Estrategias de recuperación de desastres

En el caso en que se genere un plan de emergencia, el responsable del desarrollo e implementación del plan debería ser el administrador del centro de datos. En cada área de la empresa existe un líder que sería el Jefe o Encargado del área, debido a la responsabilidad que tiene en el grupo. Éste debería sugerir al Administrador las medidas de seguridad a implementar en el plan que requiera su sector.

3.3 Diseño del Plan de Seguridad Informática

- Alcance: Este documento se aplica para todos los empleados de Mi Banco, así como a los proveedores y personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto.
- Contenido: Este Plan presenta las Políticas de Seguridad Informática cuyo contenido se agrupa en los siguientes aspectos:

1. **Seguridad Lógica:**

1.1. Identificación:

Deberá existir una herramienta para la administración y el control de acceso a los datos. Debe existir una **política formal de control de acceso** a datos donde se detalle como mínimo:

- El nivel de confidencialidad de los datos y su sensibilidad,
- Los procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas,
- Los estándares fijados para la identificación y la autenticación de usuarios.

El sistema deberá finalizar toda sesión interactiva cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá deslogear al usuario y limpiar la pantalla.

Los usuarios del sistema solamente podrán abrir una sesión de cada aplicación, y no podrán abrir dos sesiones del mismo menú en diferentes terminales ni en la misma terminal.

1.2. Autenticación:

La **pantalla de logeo** del sistema deberá mostrar los siguientes datos:

- Nombre de usuario, o Password, o Opción para cambiar la clave. Mientras el usuario está **ingresando su contraseña**, esta no debe ser mostrada por pantalla.

Cuando el **usuario logra logearse** al sistema deberán mostrarse los siguientes datos:

- Nombre de usuario,
- Fecha y hora de la última conexión, o Localización de la última conexión (Ej. número de terminal),

- Cantidad de intentos fallidos de conexión de ese ID de usuario desde la última conexión lograda.

La **aplicación para administrar los datos de usuarios** solo deberá ejecutarse en máquinas designadas del centro de cómputos.

1.3. Password

Los passwords deberán tener las siguientes características:

- Conjunto de caracteres alfa-numérico, longitud mínima de 6 y máxima de 10 caracteres.

El password deberá inicializarse como expirado para obligar el cambio. La fecha de expiración del password deberá ser de cuatro meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo. El password no deberá contener el nombre de la empresa, el nombre del usuario, ni palabras reservadas.

- Bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas.

2. Seguridad en las Comunicaciones:

2.1. Topología de Red

Se deberá asegurar la **integridad, exactitud, disponibilidad y confidencialidad** de los datos transmitidos, ya sea a través de los dispositivos de hardware, de los protocolos de transmisión, o de los controles aplicativos.

Deberá existir **documentación** detallada sobre los diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.

Deberán existir **medios alternativos de transmisión** en caso de que alguna contingencia afecte al medio primario de comunicación.

2.2. Conexiones Externas

Asegurar la definición e implementación de procedimientos pertinentes para el **control de las actividades de usuarios externos** del organismo a fin de garantizar la adecuada protección de los bienes de información de la organización. La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una **autorización de la Gerencia**. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.

Los usuarios de la organización que utilicen Internet deben recibir **capacitación específica** respecto a su funcionalidad y a los riesgos y medidas de seguridad pertinentes.

2.3. Configuración Lógica de Red

El riesgo aumenta con el número de conexiones a **redes externas**; por lo tanto, la conectividad debe ser la mínima necesaria para cumplir con los objetivos de la empresa.
El esquema de direcciones de la **red interna** no debe ser visible ante las conexiones externas. Deberá asegurarse que la **dirección IP** de la empresa sea un número variable y confidencial. Los **recursos lógicos** o físicos de los distintos **puestos de trabajo** no deben ser visibles en el resto de la red informática. Los recursos de los **servidores** serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.

3. Seguridad de las Aplicaciones

3.1. Software

✓El **sistema operativo** del servidor deberá presentar las siguientes características:

- Alta confiabilidad, equilibrio en costo y beneficio, compatibilidad e interoperatividad con los sistemas

operativos de las PC´s y demás sistemas usados en la empresa, escalabilidad, disponibilidad de software de aplicación y actualizaciones, buena administración y generación de logs,

- Buena performance, cumplir con los requerimientos funcionales impuestos por la empresa.
- Amigable con el usuario, o Disponibilidad de documentación.

3.2. Seguridad de Bases de Datos

El administrador de sistemas deberá confeccionar un **Plan de Migración** desde archivos indexados a bases de datos relacionales, una vez que el sistema esté desarrollado en su totalidad.

Los archivos indexados de la empresa, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener **controles de acceso**, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador del centro de cómputo.

3.3. Control de Aplicaciones

Deberán existir **estándares de configuración** de los puestos de trabajo, servidores y demás equipos de la red informática.

En base al estándar se deberá generar un **procedimiento** donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

Las **aplicaciones solo se actualizarán** debido al reporte de algún mal funcionamiento o a un nuevo requerimiento por parte de los usuarios o del personal del centro de cómputos.

Antes de hacer un cambio en la configuración de los servidores se deberá hacer un **backup de la configuración existente**. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.

3.4. Control de datos en las Aplicaciones

Los **datos de entrada y salida** del sistema deberán poseer controles donde se verifique su integridad, exactitud y validez.

Los datos de salida del sistema de la empresa deben restringirse con **controles lógicos**, de acuerdo a los permisos de acceso.

Deberán protegerse con **controles de acceso** las **carpetas** que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.

Se deberá utilizar un programa de **sincronización horaria** en todo el entorno de red, para asegurar la consistencia de los datos de las aplicaciones.

4. Seguridad Física

4.1. Equipamiento

Deberá existir una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la empresa.

4.2. Control de Acceso Físico al Centro de Datos

Se deberá restringir el acceso físico a las **áreas críticas** a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.

Se deberá asegurar que todos los **individuos** que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

Cualquier **persona ajena a la empresa** que necesite ingresar al centro de datos deberá anunciarse en la puerta de entrada, personal de sistemas designado deberá escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que éste concluya.

Asimismo, todo acceso deberá ser registrado en una bitácora de control, la cual debe contener los datos de la persona, fecha, hora de ingreso, hora de salida y motivo de ingreso.

4.3. Control de Acceso a Equipos

Las computadoras de la empresa deberán tener un password de administrador en el **BIOS**, que deberá gestionar el administrador del sistema.

Los servidores deberán tener una **llave de bloqueo** de hardware.

Cualquier **dispositivo externo** que no se encuentre en uso, deberá permanecer guardado bajo llave dentro del centro de cómputos.

Los **gabinetes** donde se ubican los switches de cada una de las sucursales, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado.

5. Administración del Centro de Datos

5.1. Capacitación

El **personal del centro de datos** debe mantenerse capacitado respecto de las tecnologías utilizadas en la organización. Debe **impartirse capacitación** a los usuarios finales a efectos de que puedan operar adecuadamente los recursos informáticos. El personal debe ser entrenado respecto al cumplimiento de lo especificado en la **política de seguridad** informática. Se debe entregar una copia de la misma a cada empleado.

Se debe obtener un **compromiso firmado** por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales.

5.2. Backup

Se deberá asegurar la existencia de un **procedimiento** aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se

especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.
La **periodicidad** de la generación de los resguardos debe ser acorde a la criticidad de la información y la frecuencia de cambios.

La **ubicación** de los backups debe contar con adecuadas medidas de seguridad, sin estar expuestos a las mismas contingencias que el centro de cómputo, es decir que deberán almacenarse en el exterior de la empresa, y ser transportados en un medio resistente que los proteja. Debe designarse un **responsable** y un suplente encargados de su custodia, y se generará un registro de los **movimientos** de estos medios.

6. Auditorías y Revisiones

6.1. Chequeos del Sistema

La empresa debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad de forma de asegurar la integridad, exactitud y disponibilidad de la información. Para ello deben existir:

Herramientas que registren todos los eventos relacionados con la seguridad de la información procesada por los centros de cómputo de la empresa.
Herramientas que analiza los registros generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.
Procedimientos de revisión de los eventos registrados, a cargo de un empleado designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.

Se deberán **registrar**, mediante logs de auditoría, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:

- Fecha y hora del evento, o fuente (el componente que disparó el evento), o ID del evento (número único que identifica el evento), o equipo (máquina donde se generó el evento), o usuario involucrado.

6.2. Responsabilidades de los Encargados de Seguridad

El administrador del sistema o un **encargado de auditorías** designado por él, deberá:

- Determinar qué logs se generarán, o Determinar qué eventos de seguridad se auditarán, o Determinar qué datos se recogerán de estas auditorías,
- Administrar, desarrollar e implementar los procedimientos de auditoría y revisión.
- Monitorizar y reaccionar a los avisos (warnings) y reports.
- Chequear aleatoriamente para verificar el cumplimiento de los requerimientos y procedimientos de seguridad,
- Revisar los reportes de auditorías cuando es advertido de anomalías.

6.3. Auditorías de Control de Acceso

Los **logs** deben almacenarse en carpetas de los servidores protegidas con contraseña. Esta contraseña debe ser desconocida para todos los usuarios del sistema, incluso para el administrador, por lo que debe conservarla un miembro del Directorio.

Deberán generarse logs referidos al **acceso a datos**, identificando los archivos abiertos por usuario.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Análisis de Resultados

4.1.1 Para la variable independiente

La variable independiente cuenta con 1 indicador que permite contrastar los resultados del proceso de pedidos sin la aplicación de la herramienta y como se vieron influenciados con su aplicación.

X = "Política General de Seguridad Informática"

Asignando variables al indicador

X_1= Aplicación de la "Política General de Seguridad Informática"

4.1.2 Para la variable Dependiente

El presente proyecto cuenta con 5 indicadores que permiten obtener resultados que se encuentran representados en cuadros estadísticos tanto para la preprueba como para la posprueba.

Asignando variables a los indicadores

Y_1= Porcentaje de Virus detectados y eliminados oportunamente.

Y_2 = Cantidad de parches críticos aplicados.

Y_3= Tiempo de restauración de un sistema a partir de un incidente

Y_4 = Tiempo de Respuesta para solución de un incidente

Y_5= Costo de solución por incidente

Prefijo PRE = Datos recolectados en Preprueba

Prefijo POS = Datos recolectados en Posprueba

A. Tratamiento estadístico para la Preprueba.

1. **Indicador 1 =** Porcentaje de Virus detectados y eliminados oportunamente (VDE).

   La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

   Además para garantizar que el tamaño de la muestra sea representativo al trabajo observado, se requiere un tamaño de la

muestra en la que se asegure un 95% de probabilidad de éxito y un error del 0.05.

Tabla 5: Datos para los indicadores Virus detectados y eliminados

Semana	VDE
1	2
2	4
3	3
4	2

Tabla 6: Estadística descriptiva y1 preprueba

	Y_1 PRE
Media	**2.75**
Varianza	**0.916666**
Estadístico t	**-3.415650**
T crítico	**2.35336343**

2. **Indicador 2 =** Cantidad de parches críticos aplicados

   La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

   Además para garantizar que el tamaño de la muestra sea representativo al trabajo observado, se requiere un tamaño de la muestra en la que se asegure un 95% de probabilidad de éxito y un error del 0.05.

Tabla 7: Porcentaje de parches aplicados

Semana	PPA
1	45
2	38
3	42
4	40

Tabla 8: Estadística descriptiva y2 preprueba

	Y_2 PRE
Media	40.75
Varianza	8.91666
Estadístico t	-18.08
T crítico	2.35

Indicador 3 = Tiempo de restauración de un sistema (TRI).

La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

Además para garantizar que el tamaño de la muestra sea representativo al trabajo observado, se requiere un tamaño de la muestra en la que se asegure un 95% de probabilidad de éxito y un error del 0.05.

Tabla 9: Datos para los indicadores tiempo en restaurar el sistema

Incidente	TRI
1	42
2	33
3	44
4	41
5	42
6	30
7	38
8	43
9	46
10	33
11	50
12	40
13	37
14	43
15	50

Tabla 10: Estadística descriptiva y3 preprueba

	Y_3 PRE
Media	919.6
Varianza	33436.9
Estadístico t	5.92
Valor crítico de t	1.76

3. Indicador 4 = Tiempo de respuesta a un incidente

La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

Además para garantizar que el tamaño de la muestra sea representativo al trabajo observado, se requiere un tamaño de la muestra en la que se asegure un 95% de probabilidad de éxito y un error del 0.05.

Tabla 11: Datos para el Tiempo de respuesta a un incidente

Incidente	RID
1	20
2	10
3	11
4	10
5	16
6	20
7	16
8	18
9	15
10	15
11	19
12	16
13	17
14	18
15	16

Tabla 12: Estadística descriptiva y4 preprueba

	Y_4 PRE
Media	15.8
Varianza	10.6
Estadístico t	9.1200
Valor crítico de t	1.7613

4. **Indicador 5 = Costo en atender un incidente**

La muestra utilizada en la investigación ha sido asumida por los investigadores en forma no probabilística e intencionada, tomando para ello 15 unidades de análisis, siendo la unidad de análisis proceso de seguridad de la información.

Además para garantizar que el tamaño de la muestra sea representativo al trabajo observado, se requiere un tamaño de la muestra en la que se asegure un 95% de probabilidad de éxito y un error del 0.05.

Tabla 13: Datos para el Costo en atender un incidente

Incidente	CPI
1	44
2	49
3	35
4	49
5	37
6	46
7	47
8	50
9	49
10	42
11	42
12	50
13	41
14	45
15	38

Tabla 14: Estadística descriptiva y5 Preprueba

	Y_5 PRE
Media	44.26666
Varianza	24.4952
Estadístico t	9.5618
Valor crítico de t	1.7613

B. Tratamiento estadístico de la Posprueba.

1. **Indicador 1 =** Datos para los indicadores Virus detectados y eliminados**.**

Tabla 15: Datos para los indicadores Virus detectados y eliminados Y1 Posprueba

Semana	VDE
1	18
2	11
3	11
4	6

Tabla 16: Estadística Descriptiva Y1 Posprueba

	Y_1 POS
Media	11.5
Varianza	24.3333
Estadístico t	-3.4156
Valor crítico t	2.3533

2. **Indicador 2 =** Cantidad de parches críticos aplicados (CPA).

Tabla 17: Porcentaje de parches aplicados Y2 Posprueba

Semana	PPA
1	91
2	93
3	94
4	97

Tabla 18: Estadística Descriptiva Y2 Posprueba

	Y_2 POS
Media	95.25
Varianza	9.5833
Estadístico t	-18.803
Valor crítico de t	2.353

3. **Indicador 3 =** Tiempo de restauración de un sistema (TRI).

Tabla 19: Tiempo de restauración de un sistema (TRI) Y3 Posprueba

Incidente	TRI
1	31
2	31
3	26
4	31
5	35
6	35
7	29
8	30
9	25
10	25
11	34
12	31
13	28
14	30
15	26

Tabla 20: Estadística Descriptiva Y3 Posprueba

	Y_3 POS
Media	29.8
Varianza	11.1714
Estadístico t	5.9160
Valor crítico de t	1.7613

4. **Indicador 4 =** Tiempo de respuesta a un incidente (RID)

Tabla 21: Cuadro de tratamiento de los datos recolectados para el Indicador Y4 Posprueba

Incidente	RID
1	10
2	9
3	7
4	6
5	5
6	5
7	9
8	10
9	8
10	6
11	8
12	9
13	5
14	9
15	9

Tabla 22: Estadística Descriptiva Y4 Posprueba

	Y_4 POS
Media	7.4666
Varianza	3.4095
Estadístico t	9.1200
Valor crítico de t	1.7613

5. **Indicador 5 = Costo en atender un incidente.**

Tabla 23: Costo en atender un incidente. Y5 Posprueba

Incidente	CPI
1	26
2	30
3	33
4	34
5	26
6	34
7	29
8	32
9	25
10	27

11	35
12	27
13	29
14	29
15	29

Tabla 24: Estadística Descriptiva Y5 Posprueba

	Y_5 POS
Media	**29.6666**
Varianza	**10.5238**
Estadístico t	**9.5618**
Valor crítico de t	**1.7613**

C. Comparación Estadística del Tratamiento de la Preprueba y Posprueba.

1. **Indicador 1 =** Porcentaje de Virus detectados y eliminados oportunamente (VDE)

Tabla 25: Estadística Descriptiva Y1 Preprueba y Posprueba

	Y_1 PRE	Y_1 POS
Media	**2.75**	**11.5**
Varianza	**0.9166**	**24.333**
Observaciones	**4**	**3**
Valor crítico de t	**2.3533**	

2. **Indicador 2 =** Cantidad de parches críticos aplicados (CPA).

Tabla 26: Estadística Descriptiva Y2 Preprueba y Posprueba

	Y_2 PRE	Y_2 POS
Media	**40.75**	**95.25**
Varianza	**8.9166**	**9.5833**
Observaciones	**4**	**4**
Valor crítico de t	**2.3533**	

3. **Indicador 3 =** Tiempo de restauración de un sistema (TRI).

Tabla 27: Estadística Descriptiva Y3 Preprueba y Posprueba

	Y_3 PRE	Y_3 POS
Media	40.8	29.8
Varianza	34.3142	11.1714
Observaciones	15	15
CoefPer	0.162710	

4. **Indicador 4 =** Tiempo de respuesta a un incidente (RID)

Tabla 28: Estadística Descriptiva Y4 Preprueba y Postprueba

	Y_4 PRE	Y_4 POS
Media	15.8	7.4666
Varianza	10.6	3.4095
Observaciones	15	15
CoefPer	0.12356	

5. **Indicador 5 =** Costo de un incidente (CPI)

Tabla 29: Estadística Descriptiva Y5 Preprueba y Posprueba

	Y_5 PRE	Y_5 POS
Media	44.2666	29.6666
Observaciones	15	15
Varianza	24.4952	10.5328
Estadístico t	9.56184	

4.2 Prueba de Hipótesis por Indicador

4.2.1 Validación de la hipótesis para el indicador Y1:

Porcentaje de Virus detectados y eliminados oportunamente (VDE).

Hipótesis General del Indicador

Si se aplica la Política General de Seguridad Informática entonces se influye positivamente en el Porcentaje de Virus detectados y eliminados oportunamente (VDE) en la entidad financiera MiBanco.

Hipótesis Nula

$\boldsymbol{H_0} =$ El número de virus detectados y eliminados no es significativamente menor sin la Política General de Seguridad Informática.

Hipótesis Alterna

$\boldsymbol{H_a} =$ El número de virus detectados y eliminados es significativamente menor sin la Política General de Seguridad Informática.

Hipótesis Estadística

Sean:

μ_1= Media de los Porcentaje de Virus detectados y eliminados oportunamente de la preprueba.

μ_2 = Media de los Porcentaje de Virus detectados y eliminados oportunamente de la posprueba.

H_0: $\mu_1 \leq \mu_2$

H_a: $\mu_1 > \mu_2$

Tabla 30: Cantidad de virus detectados y eliminados

Cantidad de virus detectados y eliminados		
	Variable 1	*Variable 2*
Media	2.75	11.5
		24.333333
Varianza	0.91666667	3
Observaciones	4	4
Coeficiente de correlación de Pearson	-0.1058677	
Diferencia hipotética de las medias	0	
Grados de libertad	3	
Estadístico t	-3.41565026	
P(T<=t) una cola	0.02098823	
Valor crítico de t (una cola)	2.35336343	

Interpretación:

De la tabla se desprende que, el estadístico t= - 3.41565026, es significativamente menor que el t crítico = 2.35336343, por lo que cae en la zona de aceptación de la Ha; a favor de los resultados con la Política General de Seguridad Informática.

4.2.2 Validación de la hipótesis para el indicador Y2:

Cantidad de parches críticos aplicados (CPA).

Hipótesis General del Indicador.

Si se aplica la Política General de Seguridad Informática, entonces se influye positivamente en la Cantidad de parches críticos aplicados (CPA) en el soporte centralizado de la entidad Financiera Mi Banco.

Hipótesis Nula

$\boldsymbol{H_0}$ = El porcentaje de parches críticos aplicados, no es significativamente menor sin la Política General de Seguridad Informática.

Hipótesis Alterna

$\boldsymbol{H_a}$ = El porcentaje de parches críticos aplicados, es significativamente menor sin la Política General de Seguridad Informática.

Hipótesis Estadística

Sean:

μ_1= Media de Cantidad de parches críticos aplicados de la preprueba.

μ_2 = Media de Cantidad de parches críticos aplicados de la posprueba.

H_0: $\mu_1 \leq \mu_2$

H_a: $\mu_1 > \mu_2$

Tabla 31: Porcentaje de Parches críticos aplicados

Porcentaje de parches críticos aplicados

	Variable 1	*Variable 2*
Media	40.75	95.25
Varianza	8.91666667	9.58333333
Observaciones	4	4
Coeficiente de correlación de Pearson	-0.96459047	
Diferencia hipotética de las medias	0	
Grados de libertad	3	
Estadístico t	-18.0831413	
P(T<=t) una cola	0.00018444	
Valor crítico de t (una cola)	2.35336343	

Interpretación:

De los resultados de la prueba t, se desprende que el estadístico t = -18.08, es significativamente menor que el t crítico = 2.35, por lo cual se acepta la hipótesis alterna para el tiempo de restauración del sistema.

4.2.3 Validación de la hipótesis para el indicador Y3:

Tiempo de restauración de un sistema (TRI).

Hipótesis General del Indicador.

Si se aplica la Política General de Seguridad Informática, entonces se influye positivamente en el Tiempo de restauración de un sistema (TRI) en la entidad Financiera Mi Banco.

Hipótesis Nula

H_0 = El tiempo de restauración de un sistema no es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Alterna

H_a = El tiempo de restauración de un sistema es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Estadística

μ_1= Media del Tiempo de restauración de un sistema en la preprueba.

μ_2 = Media del Tiempo de restauración de un sistema en la posprueba.

H_0: $\mu_1 \leq \mu_2$

H_a: $\mu_1 > \mu_2$

Tabla 32: Tiempo de Restauración de un incidente

Tiempo de Restauración de un incidente

	Variable 1	*Variable 2*
Media	40.8	29.8
Varianza	34.3142857	11.1714286
Observaciones	15	15
	-	
Coeficiente de correlación de Pearson	0.16271028	
Diferencia hipotética de las medias	0	
Grados de libertad	14	
Estadístico t	5.91607978	
P(T<=t) una cola	1.8809E-05	
Valor crítico de t (una cola)	1.76131012	

Interpretación:

De los resultados de la prueba t, se desprende que el estadístico t = 5.92, es mayor que el t crítico = 1.76, por lo cual se acepta la hipótesis alterna para el tiempo de restauración del sistema; lo que es lo mismo que el nivel de significancia p= 0.05 es mayor que el p=0.000018809 de la prueba aceptándose igualmente la hipótesis alterna.

4.2.4 Validación de la hipótesis para el indicador Y4:

Tiempo de respuesta a un incidente (RID)

Hipótesis General del Indicador.

Si se aplica la Política General de Seguridad Informática, entonces se influye positivamente en el Tiempo de respuesta a un incidente (RID) en la Entidad Financiera Mi Banco.

Hipótesis Nula

$\boldsymbol{H_0}$ = El tiempo de respuesta a un incidente no es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Alterna

$\boldsymbol{H_a}$ = El tiempo de respuesta a un incidente es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Estadística

μ_1= Media del Tiempo de respuesta a un incidente de la preprueba.

μ_2 = Media del Tiempo de respuesta a un incidente de la posprueba.

H_0: $\mu_1 \leq \mu_2$

H_a: $\mu_1 > \mu_2$

Tabla 33: Tiempo en responder a un incidente

Tiempo en responder a un incidente		
	Variable 1	*Variable 2*
Media	15.8	7.46666667
Varianza	10.6	3.40952381
Observaciones	15	15
Coeficiente de correlación de Pearson	0.12356785	
Diferencia hipotética de las medias	0	
Grados de libertad	14	
Estadístico t	9.12002768	
P(T<=t) una cola	1.4435E-07	
Valor crítico de t (una cola)	1.76131012	

Interpretación:

De los resultados de la prueba t, se desprende que el estadístico t = 9.12, es mayor que el t crítico = 1.76, por lo cual se acepta la hipótesis alterna para el tiempo en responder a un incidente; lo que es lo mismo que el nivel de significancia p= 0.05 es mayor que el p=0.000014435 de la prueba aceptándose igualmente la hipótesis alterna.

4.2.5 Validación de la hipótesis para el indicador Y5:

Costo de un incidente (CPI)

Hipótesis General del Indicador.

Si se aplica la Política General de Seguridad Informática entonces se influye positivamente en el Costo de un incidente (CPI) en la entidad Financiera Mi Banco.

Hipótesis Nula

H_0 = El costo en solucionar un incidente no es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Alterna

H_a = El costo en solucionar un incidente es significativamente menor con la Política General de Seguridad Informática.

Hipótesis Estadística

Sean:

μ_1 = Media del Costo de un incidente de la preprueba.

μ_2 = Media del Costo de un incidente de la posprueba.

H_0: $\mu_1 \leq \mu_2$

H_a: $\mu_1 > \mu_2$

Tabla 34: Costo en solucionar un incidente

Costo en solucionar un incidente		
	Variable 1	Variable 2
Media	44.2666667	29.6666667
Varianza	24.4952381	10.5238095
Observaciones	15	15
Coeficiente de correlación de Pearson	0.00148294	
Diferencia hipotética de las medias	0	
Grados de libertad	14	
Estadístico t	9.56184718	
P(T<=t) una cola	8.1122E-08	
Valor crítico de t (una cola)	1.76131012	

Interpretación:

De los resultados de la prueba t, se desprende que el estadístico t = 9.56, es mayor que el t crítico = 1.76, por lo cual se acepta la hipótesis alterna para el costo en solucionar un incidente; lo que es lo mismo que el nivel de significancia p= 0.05 es mayor que el p=0.000081122 de la prueba aceptándose igualmente la hipótesis alterna.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

A continuación se presentan las conclusiones y recomendaciones obtenidas en el desarrollo del presente trabajo de investigación.

5.1 Conclusiones

De la investigación realizada hemos obtenido las siguientes conclusiones:

5.1.1 La Política General de Seguridad Informática, en la entidad Financiera Mi Banco, no se está aplicando por lo que la información no está segura y no se tiene aún conciencia de lo delicado que representaría una eventual pérdida o daño de la información.

5.1.2 En relación a los resultados de las hipótesis para cada uno de los indicadores, prueba que la Política General de Seguridad Informática, beneficia a la entidad Financiera Mi Banco, en este punto todos los indicadores tomados para el estudio han sido validados según las hipótesis propuestas:

1. El número de virus detectados y eliminados son mayores con la Política General de Seguridad Informática como se muestran en la medias 2.75 y 11.5 para la preprueba y posprueba respectivamente.
2. La cantidad de parches críticos aplicados son mayores con la Política General de Seguridad Informática, según como se muestra con las medias de 40.75 y 95.25 para la preprueba y posprueba respectivamente.
3. El tiempo demandado en la restauración de un sistema es mucho menor con la Política General de Seguridad Informática, como se muestra con las medias de 40.8 y 29.8 respectivamente para la pre y posprueba.
4. El tiempo de respuesta para un incidente es mucho menor con la Política General de Seguridad Informática, como se muestra con las medias 15.8 y 7.47 para la preprueba y posprueba respectivamente.
5. El costo que demanda solucionar un incidente es mucho menor con la Política General de Seguridad Informática, como se muestra en las medias 44.27 y 29.67 para la preprueba y posprueba respectivamente.

5.1.3 A medida que se llevó a cabo la presente investigación (más aun al finalizar con el documento), los funcionarios de la empresa MiBanco, pudieron comprender e interiorizar la importancia que tenía la información, y la manera cómo se encontraba expuesta. En ese sentido, valoraron y aprobaron la implantación de la Política de Seguridad de Informática, con la finalidad de ayudar a mitigar los riesgos de seguridad a los que todas las empresas de cualquier rubro y a nivel mundial, enfrentan en la actualidad.

5.1.4 La aplicación de la Política de Seguridad Informática será entonces, un primer paso para una adecuada Gestión de Seguridad de la Información, la cual abarca a la información en cualquier de sus formas (virtual, escriba, hablada, entre otros). Cabe indicar que cuando se llegue a este nivel, se recomendó a la empresa, desvincular esta gestión del departamento de tecnología, ya que es necesario e indispensable que exista un ente independiente que se encargue de verificar la existencia y ejecución de los controles.

5.2. Recomendaciones

La prueba de aplicación de la Política General de Seguridad Informática ha demostrado que su aplicación es beneficiosa para la entidad Financiera Mi Banco, sin embargo es pertinente hacer las siguientes recomendaciones:

1) Que la entidad financiera Mi Banco, siga aplicando la Política General de Seguridad de la Información propuesta.

2) Para un mejor control de la aplicación de la Política General de Seguridad Informática, se recomienda evaluar diversos software para help desk, service desk y cualquiera que tenga la posibilidad de controlar la provisión de los servicios de TI en la empresa.

3) Capacitar al personal del área de Sistemas, en control y aseguramiento de planes de seguridad informática.

4) Adicionalmente se propone que se lleven a cabo auditorías periódicas que puedan determinar la efectividad de los controles implamantados.

BIBLIOGRAFÍA

Libros:

1. John, Hayman. investigación y solución . Buenos Aires : Editorial Paidos, 1969.
2. Sabino, Deza Jaime y Muñoz. Metodología de la Investigación Científica. Perú : Ediciones Universidad Alas Peruanas, 2008. p.13.
3. Hernandez Sampieri, Roberto. Metodología de la Investigación. 4ta Edición. México. 2006. Mc Graw Hill. pp.
4. Alejandro Hernández Trasobares, Los Sistemas de Información: evolución y desarrollo, Zaragoza 2004.
5. Fundamentos de Marketing, de Stanton, Etzel y Walker, 13va Edición, pp. 604 al 607.
6. Campderrich Falgueras, Benet. Ingeniería de Software. 1ra ed., España, Ed. UOC, 2003, pág. 83 de 320 pp.
7. Weitzenfeld Alfredo. Ingeniería de software orientada a objetos con UML. 1ra ed., España, Ed. Thomson, 2003, pág 275 de 705 pp.
8. Campderrich Falgueras, Benet. Ingeniería de Software. 1ra ed., España, Ed. UOC, 2003, pág. 99 de 320 pp.
9. Weitzenfeld, Alfredo. Ingeniería de software orientada a objetos con UML. 1ra ed., España, Ed. Thompson, 2003, pág 71 de 705 pp.

Artículos de Internet:

1. Innovación, http://www.innovacion.org.gt/content/la-innovacion-y-tecnologia-estrategias-fundamentales-casos-de-exito
2. Microsoft, http://www.microsoft.com/spain/compare/casestudies/cs-lse.mspx
3. Lap ware, http://labware.es/category/casos-de-exito/
4. Disponible en URL http://www.monografias.com/
5. “Order promising” y Gestión de Pedidos: una visión de procesos, http://adingor.es/congresos/web/uploads/cio/cio2005/prod_gest_operaciones/43.pdf
6. G., Tevni Grajales. [En línea] http://tgrajales.net/investipos.pdf.

7. G., Tevni Grajales. [En línea] http//es.crebd.com/doc/15246394/Tipos y Niveles Investigación 2009.
8. Raúl Dominguez, “Sistema de Información para la Gestión de Venta de Ropa en el Puesto Comercial Raúl Indepencia 2012”, en: http://www.buenastareas.com/ensayos/Sistema-De-Informaci%C3%B3n-Para-La-Gestion/5752957.html
9. José Benjamín Gonzales Vega, “Propuesta de un modelo de Gestión de Pedidos para la planeación de la producción y distribución en la empresa chantilly, s.a. de c.v.”, en: http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/6485/1/C7.1429.pdf
10. Cristian Gonzalo Karolys Tovar, Diego Francisco Niama Bonifaz, **“**Implementación de un Prototipo para Gestión de Productos y Pedidos en Distribuidoras utilizando SMS de Tecnología GSM**”,** 2009, en: http://repositorio.espe.edu.ec/handle/21000/470
11. Bach. Fajardo Acosta Melvin, Bach. Muga Rivera Juna José, **“**Desarrollo e Implementación de un Sistema de Gestión Comercial para mejorar la rentabilidad de la empresa OLEOCENTRO EICOL E.I.R.L.”, 2009, en: http://www.slideshare.net/carloschavezmonzon/tesis-sobre-la-metodologa-mipe
12. Bach. Neira Lázaro Cynthia Dajana, Bach. Ortecho Alva Jorge Luis, “Sistema Informático con Hand Held para captura de Datos en la toma de Pedidos y Cobranza de la empresa del Manantial SAC”, 2007, en: http://repositorio.espe.edu.ec/bitstream/21000/470/1/T-ESPE-024461.pdf
13. Buenas Tareas, http://www.buenastareas.com/ensayos/Evoluci%C3%B3n-De-Las-Tecnolog%C3%ADas-De-La/589550.html
14. Gestión Comercial, http://www.eumed.net/libros/2009a/504/Gestion%20comercial.htm
15. Ufg,http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/658.022-B715p/658.022-B715p-Capitulo%20II.pdf
16. Principios de Sistemas de Información: Enfoque Administrativo - Ralph M. Stair, George Walter Reynolds, George W. Reynolds – pp.4, http://books.google.com.pe/books?id=k_sKKIF0iCgC&printsec=frontcover&dq=sistemas+de+informacion&hl=es&sa=X&ei=xgvET4CJMufG6AGFocXNCg&ved=0CDEQ6AEwAA#v=onepage&q=sistemas%20de%20informacion&f=false

17. Armando Duany Dangel - Centro de Estudio de Desarrollo Agrario y Rural. http://www.econlink.com.ar/sistemas-informacion/definicion

18. Oliver Eduardo Martínez Pelayo, Categoría nueva economía, internet y tecnología 11-2004, Factores clave de éxito: sistemas y tecnologías de información; ventajas y problemáticas en la industria, http://www.gestiopolis.com/canales3/ger/gertecventdes.htm

19. Principios de Sistemas de Información: Enfoque Administrativo - Ralph M. Stair, George Walter Reynolds, George W. Reynolds – pp. 15-16 http://books.google.com.pe/books?id=k_sKKIF0iCgC&printsec=frontcover&dq=sistemas+de+informacion&hl=es&sa=X&ei=xgvET4CJMufG6AGFocXNCg&ved=0CDEQ6AEwAA#v=onepage&q=sistemas%20de%20informacion&f=false

20. Armando Duany Dangel - Centro de Estudio de Desarrollo Agrario y Rural, http://www.econlink.com.ar/sistemas-informacion/clasificacion

21. Aspectos Organizacionales de los Sistemas de Información: tipos de sistemas de información. http://fccea.unicauca.edu.co/old/tiposdesi.htm

22. Wilber Calles, http://wilbercalles.tripod.com/impyben.html

23. Berenice Betancourt ,Ventajas y desventajas de utilizar sistemas de información, México, 10 de Mayo de 2011 http://www.queo.mx/index.php?option=com_content&view=article&id=8021&catid=4:ciencia-y-tecnolog&Itemid=12

24. Gestión, http://www.guiaempresaxxi.com/gestion/docs-definicion-de-gestion-comercial.html

25. Ivan Thompson, Proceso de Venta Agosto 2005. http://www.promonegocios.net/mercadotecnia/proceso-venta.htm

26. Buenas tareas, http://www.buenastareas.com/ensayos/Gestion-De-Pedido/2663535.html

27. Educared, http://www.educared.org/global/anavegar6/podium/E/598/webdocupedido.html

28. Cueva Lovelle, Juan Manuel. Introducción de UML. En: http://lsm.dei.uc.pt/ribie/docfiles/txt20037292220Uso%20de%20la%20notacion%20UML.pdf, España, 1999, pág. 15 de 109 pp.

29. Cáceres Tello, Jesús. Diagrama de Casos de Uso. En: http://www2.uah.es/jcaceres/uploaded/capsulas/DiagramaCasosDeUso.pdf,España, 2008, 4 pp.

GLOSARIO DE TERMINOS

1. **Almacenamiento**: Para cualquier sistema ordenado, las unidades de almacenamiento son aquellas que permiten guardar física o virtualmente archivos de datos de todo tipo.

2. **Análisis**: Un análisis es el acto de separar las partes de un elemento para estudiar su naturaleza, su función y/o su significado.

3. **Codificación:** Es aquella operación que tiene lugar para enviar datos de un lugar a otro, procesarlos y obtener resultados a partir de ellos.

4. **Control:** Es la medición de los resultados actuales y pasados en relación con los esperados, con el fin de corregir, mejorar y formular nuevos planes.

5. **Eficiencia:** Se refiere particularmente a hacer las operaciones en el menor tiempo, utilizando adecuadamente los recursos y reduciendo costos.

6. **Fase:** Cada uno de los estados sucesivos de una cosa que cambia o se desarrolla.

7. **Información**: Datos que tienen significado para determinados colectivos. La información resulta fundamental para las personas, ya que a partir del proceso cognitivo de la información que obtenemos continuamente con nuestros sentidos vamos tomando las decisiones que dan lugar a todas nuestras acciones.

8. **Procedimiento:** Manera específica de efectuar una actividad.

9. **Procesamiento:** el procesamiento supone la transformación de datos en salidas útiles.

10. **Proceso:** conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado.

11. **Reportes:** Es aquel documento que se utilizará cuando se quiera informar o dar noticia acerca de una determinada cuestión.

12. **Seguridad Informática:** Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

13. **Sistemas de Información:** es un conjunto de componentes interrelacionados para recolectar, manipular y diseminar datos e información y para disponer de un mecanismo de retroalimentación útil en el cumplimiento de un objetivo.

14. **Software:** Se le conoce así al equipamiento lógico o soporte lógico de una computadora digital.

15. **Tecnología**: Aplicación de los conocimientos científicos para facilitar la realización de las actividades humanas. Supone la creación de productos, instrumentos, lenguajes y métodos al servicio de las personas.

16. **Tecnologías de la Información y la Comunicación**(TIC) : Cuando unimos estas tres palabras hacemos referencia al conjunto de avances tecnológicos que nos proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, Internet, la telefonía, los "mas media", las aplicaciones multimedia y la realidad virtual. Estas tecnologías básicamente nos proporcionan información, herramientas para su proceso y canales de comunicación.

ANEXOS

Anexo 1: Historia

Anexo 2 Objetivos

Anexo 3: DR - Formato Planes y Entregables 2015 – Proyectos 3.0

I. Gestión de Proyectos	Cumplimiento

Tema	Detalle	Inicio	Término	Responsable	M14 - E	M14 - R	Cump.
1. Proyectos Normativos							
1.1 Ley de Protección de Datos Personales - SI							
	Definición de Alcance y Objetivo	01/07/2015	30/07/2015	LOV			
	Desarrollo	01/08/2015	30/12/2015	LOV			
	Documentación y Adecuación Normas Internas	01/09/2015	30/11/2015	LOV			
	Coordinación con Sistemas e Implementación	01/08/2015	30/12/2015	LOV			
	Capacitación y Despliegue	01/12/2015	30/12/2015	LOV			
1.2 Reglamento de Tarjetas de Crédito y Débito - SI							
	Definición de Alcance y Objetivo	01/08/2015	30/08/2015	JMM			
	Desarrollo	01/08/2015	30/12/2015	JMM			
	Documentación y Adecuación Normas Internas	01/10/2015	30/12/2015	JMM			
	Coordinación con Sistemas e Implementación	01/10/2015	30/12/2015	JMM			
	Capacitación y Despliegue	01/12/2015	30/12/2015	JMM			
2. Proyectos Corporativos							
3. Proyectos para Gestión / Resultados							
3.1 Proyecto ASA							

	Definición de Alcance y Objetivo	01/02/2015	28/02/2015	CSL			
	Desarrollo	01/03/2015	31/12/2015	CSL			
	Documentación y Adecuación Normas Internas	-	-				
	Coordinación con Sistemas e Implementación	01/01/2016	31/03/2016	CSL			
	Capacitación y Despliegue	-	-				
3.2	**Administración de eventos de seguridad (ENVISION)**						
	Definición de Alcance y Objetivo	01/11/2015	30/11/2015	RSS			
	Desarrollo	01/12/2015	30/04/2016	RSS			
	Documentación y Adecuación Normas Internas	01/04/2016	30/05/2016	RSS			
	Coordinación con Sistemas e Implementación	01/12/2015	30/04/2016	RSS			
	Capacitación y Despliegue	01/05/2016	30/05/2016	RSS			
3.3	**Seguridad en base de datos (IMPERVA)**						
	Definición de Alcance y Objetivo	01/04/2015	30/07/2015	RSS			
	Desarrollo	01/07/2015	**30/04/2016**	RSS			
	Documentación y Adecuación Normas Internas	01/10/2015	**30/04/2016**	RSS			
	Coordinación con Sistemas e Implementación	01/07/2015	**30/04/2016**	RSS			
	Capacitación y Despliegue	01/10/2015	**30/04/2016**	RSS			
3.4	**Seguridad perimetral**						
	Definición de Alcance y Objetivo	01/03/2015	28/03/2015	JMM			
	Desarrollo	01/04/2015	30/08/2015	JMM			
	Documentación y Adecuación Normas Internas	01/06/2015	30/08/2015	JMM			
	Coordinación con Sistemas e Implementación	01/05/2015	30/08/2015	JMM			
	Capacitación y Despliegue	01/06/2015	30/08/2015	JMM			
3.5	**Segregación de funciones en TOPAZ - Fase 2**						
	Definición de Alcance y Objetivo	01/07/2015	30/07/2015	HLL			
	Desarrollo	01/08/2015	30/12/2015	HLL			
	Documentación y Adecuación Normas Internas	01/11/2015	30/12/2015	HLL			
	Coordinación con Sistemas e Implementación	-	-	HLL			
	Capacitación y Despliegue	-	-	HLL			

Anexo 4: Gestión de Entregables

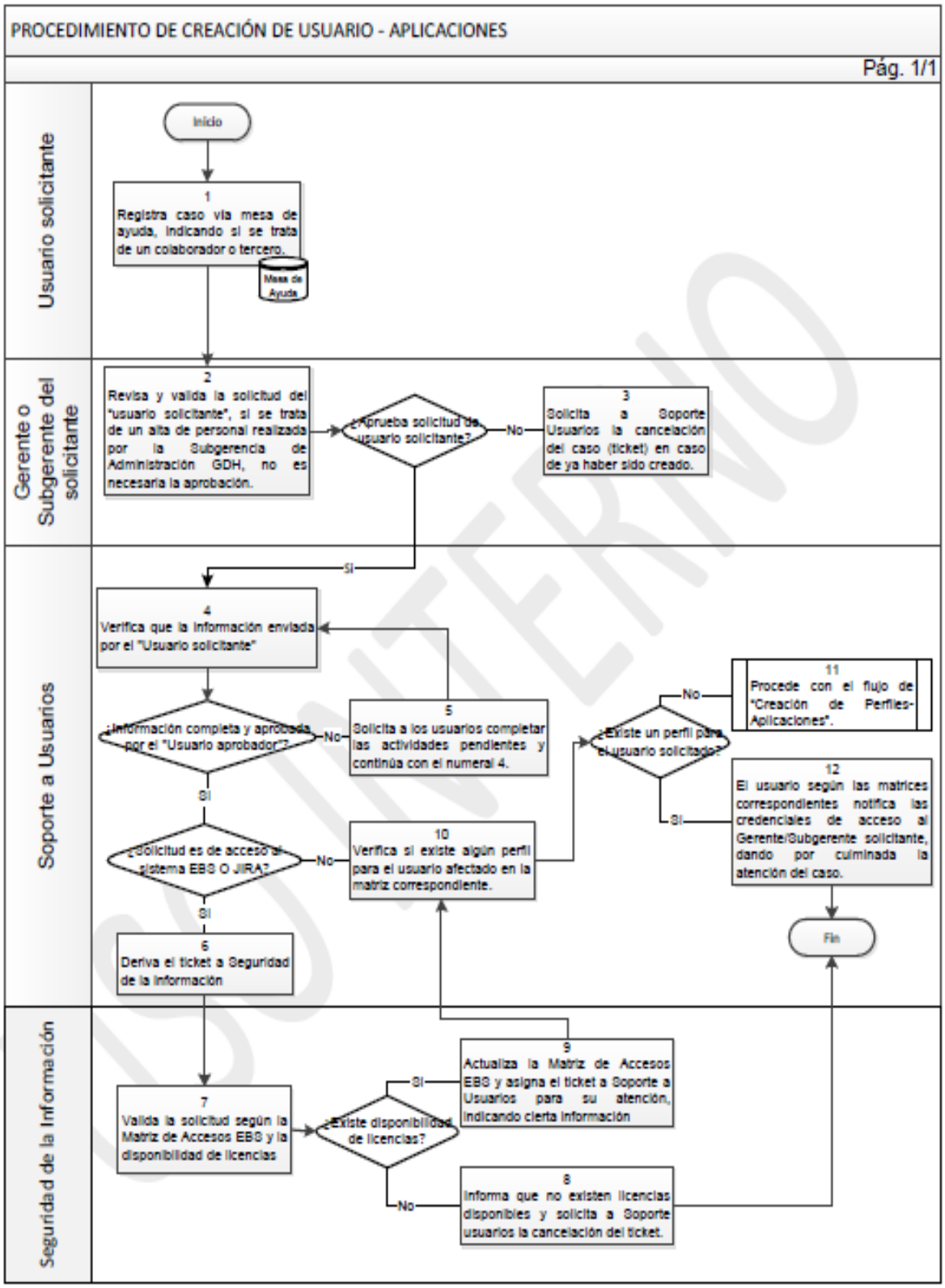
II. Gestión de Entregables

Reporte / Informe	Destino	Periodicidad	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
1. Reportes / Informes Normativos														
Informe Anual - Gestión SI (EDYFICAR)	Directorio	A	X											
Informe Anual - Gestión SI (MIBANCO)	Directorio	A	X											
IGROP - Gestión de Seguridad de la Información (EDYFICAR)	SBS	A	X											
IGROP - Gestión de Seguridad de la Información (MIBANCO)	SBS	A	X											
2. Reportes / Informes Corporativos														
Informe del Programa Corporativo de Seguridad de la Información	BCP	C				X				X				X
Informe del Alineamiento Corporativo de Riesgo Operacional	BCP	M	X	X	X	X	X	X	X	X	X	X	X	X
3. Reportes / Informes Gestión Resultados														
Informe Anual de Gestión de Activos	CAR	A							X					
Informe Anual de Evaluación de Riesgos	CAR	A												X
Informe Mensual - Gestión SI	CAR	M	X	X	X	X	X	X	X	X	X	X	X	X
Informe Mensual - Gestión SI (CTRO)	CTRO	M	X	X	X	X	X	X	X	X	X	X	X	X
Informe Mensual - Gestión SI (CGRO)	CGRO	T	X			X			X			X		

Anexo 5: Lineamientos Específicos de Control de Accesos

Lineamiento	Active Directory	TOPAZ	EBS	ADRYAN C/S	TRADER LIVE	ICS
Número de intentos de contraseña errada	05	03	03	03	03	3
Número de últimas contraseñas que no se pueden repetir	06	06	No aplica	06	03	No Aplica
Longitud mínima de la contraseña	08	08	08	08	08	08
Tiempo de caducidad de la contraseña	45 días	30 días	90 días	90 días	90 días	90 días
Número de días previos de aviso antes que una contraseña caduque	05 días	07 días	No aplica	15 días	15 días	No Aplica
Tiempo de inactividad de las sesiones de trabajo	10 minutos	10 minutos	30 min	30 min	No aplica	35
Tiempo mínimo requerido para que una contraseña pueda ser reutilizada nuevamente	No aplica	06 meses	06 meses	6 meses	No aplica	No Aplica
Soporta complejidad en la definición de la contraseña	Habilitado	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado	No Aplica

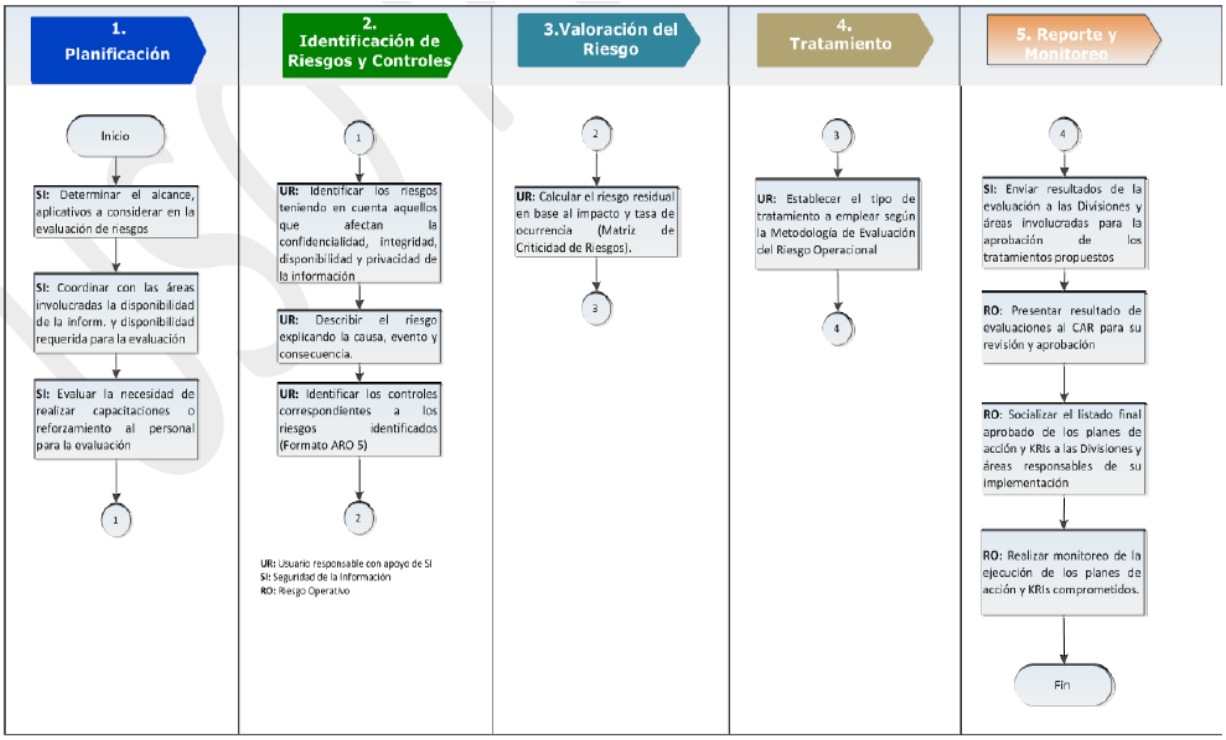
Anexo 6: Procedimiento de Creación de Usuario - Aplicaciones



Anexo 7: Matriz de Responsabilidades

Nro.	Responsable	Descripción
1.	Usuario Solicitante	Registra caso vía mesa de ayuda, indicando si se trata de un colaborador (Matricula, Nombre, Apellido, Cód. Cargo, cargo, recurso solicitado, no incluye las solicitudes de Administración GDH, responsabilidades solicitadas) y para el caso de tercero(DNI, Nombres, Apellidos, Empresa, Recurso solicitado, Gerente/Subgerente responsable del proveedor, fecha de expiración, máximo 3 meses para externos y 6 meses para outsourcing, ambos renovables).
2.	Gerente o Subgerente del solicitante	Revisa y valida la solicitud del "usuario solicitante", si se trata de un alta de personal realizada por la Subgerencia de Administración GDH, no es necesaria la aprobación.
	Gerente o Subgerente del solicitante	**¿Aprueba solicitud de usuario solicitante?** No, continua actividad 4 Si, continua actividad 3
3.	Gerente o Subgerente del solicitante	Solicita a Soporte Usuarios la cancelación del caso (ticket) en caso de ya haber sido creado.
4.	Soporte a Usuarios	Revisa y valida la solicitud del "usuario solicitante". **Nota**: Si se trata de un alta de personal realizada por la Subgerencia de Administración GDH, no es necesaria la aprobación.
	Soporte a Usuarios	**¿Información completa y aprobada por el "Usuario aprobador"?** No, continua con la actividad 5 Si, continúa con la siguiente condición.
5.	Soporte a Usuarios	Solicita a los usuarios completar las actividades pendientes y continúa con el numeral 4.
	Soporte a Usuarios	**¿Solicitud es de acceso al sistema EBS O JIRA?** No, continua actividad 10 Si, continua actividad 6
6.	Soporte a Usuarios	Deriva el ticket a Seguridad de la Información
7.	Seguridad de la Información	Valida la solicitud según la Matriz de Accesos EBS y la disponibilidad de licencias

Anexo 8: ESQUEMA DE TRABAJO



Anexo 9: Modelo de Casos de Uso