UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

ELECTRÓNICA E INDUSTRIAL

Carrera de Ingeniería en Sistemas Computacionales e Informáticos

TEMA:

"NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA."

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniera en Sistemas Computacionales e Informáticos.

AUTOR: Tania Verónica Guachi Aucapiña.

TUTOR: Ing. David Guevara.

Ambato - Ecuador

Julio 2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: Norma de Seguridad Informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.", de la señorita Tania Verónica Guachi Aucapiña, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos., de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato, Julio del 2012

EL TUTOR

Ing. David Guevara

AUTORÍA

El presente trabajo de investigación: "Norma de Seguridad Informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor**.**

Ambato, Julio del 2012

……..

Tania Verónica Guachi Aucapiña

CC: 180448895-3

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes, Ing. M.Sc. Oswaldo Paredes, Ing. Francisco López, Ing. Luis Solís, revisó y aprobó el Informe Final del trabajo de graduación titulado "NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.", presentado por la señorita Tania Verónica Guachi Aucapiña de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

……..

Ing. Oswaldo Paredes

PRESIDENTE DEL TRIBUNAL

……

Ing. Francisco López

DOCENTE CALIFICADOR

..……

Ing. Luis Solís

DOCENTE CALIFICADOR

DEDICATORIA

Con amor y afecto más profundo a las razones de mi vida: Dios, mis Padres, Hermanos, porque con amor, paciencia, sabiduría y fortaleza que ellos me han ofrecido inspiran cada momento de mi vida.

Tania

AGRADECIMIENTO

A Dios por darme salud, vida y fortaleza para cumplir con esta meta.

A mis padres Carmen y Samuel por ser el pilar fundamental de apoyo, amor, confianza, por los consejos brindados y los empujes para seguir adelante día tras día.

A mis Hermanos por ser un motivo más de superación

A todos mis amigos, los cuales compartimos grandes momentos en el viaje de esta carrera.

Gracias al Ing. Diego Torres jefe de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., y al Ing. David Guevara por ser guía y compartir sus conocimientos y desempeñar con satisfacción mi profesión.

Tania

INDICE

CONTENIDO **PAGINA**

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

CAPITULO II

MARCO TEÓRICO

CAPITULO III

METODOLOGÍA

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITUO VI

PROPUESTA

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

Dada la evolución de la Tecnología de la información y su relación directa con los objetivos del negocio de las Organizaciones, el universo de amenazas y vulnerabilidades crece por lo tanto es necesario proteger uno de los activos más importantes de la Organización, la información, garantizando siempre la disponibilidad, la confidencialidad e integridad de la misma. La forma más adecuada para proteger los activos de información es mediante una correcta gestión del riesgo, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos.

El Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda., es un pilar fundamental para la Cooperativa ya que opera y gestiona los sistemas de información y de comunicación por lo tanto deben brindar seguridad y confiabilidad de los mismos y así satisfacer a los usuarios de los sistemas de información, es por ello que se ha adoptado el uso de estándares para mejorar y mantener la seguridad de la información.

El presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

INTRODUCCIÓN

El propósito de la presente investigación es elaborar una solución informática que mantenga y mejore la seguridad de los sistemas de información y comunicación en la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., basada en el estándar ISO 27001.

La investigación se ha elaborado de acuerdo a la organización de información que se detalla a continuación:

En el capítulo I "EL PROBLEMA DE INVESTIGACIÓN", se identifica el problema a investigar, además se plantea la justificación y los objetivos. Es decir el marco referencial, se expone la situación actual en cuanto a los riesgos identificados que afectan a la información, por lo que es de mayor importancia adoptar medidas de seguridad para proteger la información.

En el capítulo II "MARCO TEÓRICO", se presentan los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables de la hipótesis.

En el capítulo III "METODOLOGÍA", se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

En el capítulo IV "ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS", se aplican los instrumentos de recolección de información en este caso la entrevista para determinar las condiciones actuales en cuanto a la seguridad de la información, luego de eso se procede al análisis e interpretación de los resultados de la información obtenida.

En el capítulo V "CONCLUSIONES Y RECOMENDACIONES", se presenta las conclusiones y recomendaciones del análisis e interpretación de los resultados realizados en el capitulo anterior.

En el capítulo VI "PROPUESTA", se presenta el desarrollo de la propuesta ante el problema investigado. Es decir la aplicación del Estándar ISO 27001 en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema

Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

1.2 Planteamiento del Problema

1.2.1 Contextualización:

En la actualidad los sistemas de información y comunicación son usados por diversas empresas, organizaciones e instituciones que existen mundialmente; convirtiéndose en un fenómeno social mediante un imparable proceso de comercialización. En la mayoría de las empresas e instituciones, sus sistemas de información son los activos por excelencia, imprescindibles para su propia existencia y supervivencia; de esta manera reconocen el grado de criticidad que los sistemas de información representan para su funcionamiento y el alto grado de vulnerabilidad inherente a la propia naturaleza de los mismos, y lo que es más grave, la insuficiencia de las políticas y normas de seguridad implantadas a la fecha. Con frecuencia somos testigos y/o víctimas de ataques de virus, de crackers, e incluso de empleados o usuarios maliciosos que acceden a información confidencial y la utilizan de forma perjudicial para la empresa. En muchas ocasiones somos conscientes de los daños causados cuando es demasiado tarde o quizá nunca.

En el Ecuador se encuentran instituciones que procesan datos a través de sistemas de información y comunicaciones muchas veces no tienen un buen desempeño, ni las seguridades necesarias, ni una correcta utilización de los mismos, por lo que se requiere implementar una serie de mecanismos para mejorar el uso y la disponibilidad de los mismos. Las instituciones tanto públicas como privadas en una gran mayoría manejan su información por medios de comunicaciones, así logran tener conectividad e interrelacionarse ya sea con otras o con sus clientes ahorrando de esta manera tiempo y recursos económicos. En nuestra provincia una gran mayoría de organizaciones trabaja con sistemas de información y comunicación, pero en algunas no disponen de controles adecuados para asegurar y mantener la confidencialidad, integridad y disponibilidad de los mismos.

La Cooperativa de Ahorro y Crédito "San Francisco" Ltda., es una Institución que cada vez es más consciente que la información que se maneja debe estar bien protegida, así también de ser capaces de identificar y gestionar los riesgos de seguridad de la información y esto se lleva a cabo a través de la definición de un Sistema de Gestión de Seguridad de la Información mediante de la implementación de la norma de seguridad informática ISO 27001.

1.2.2 Árbol del Problema

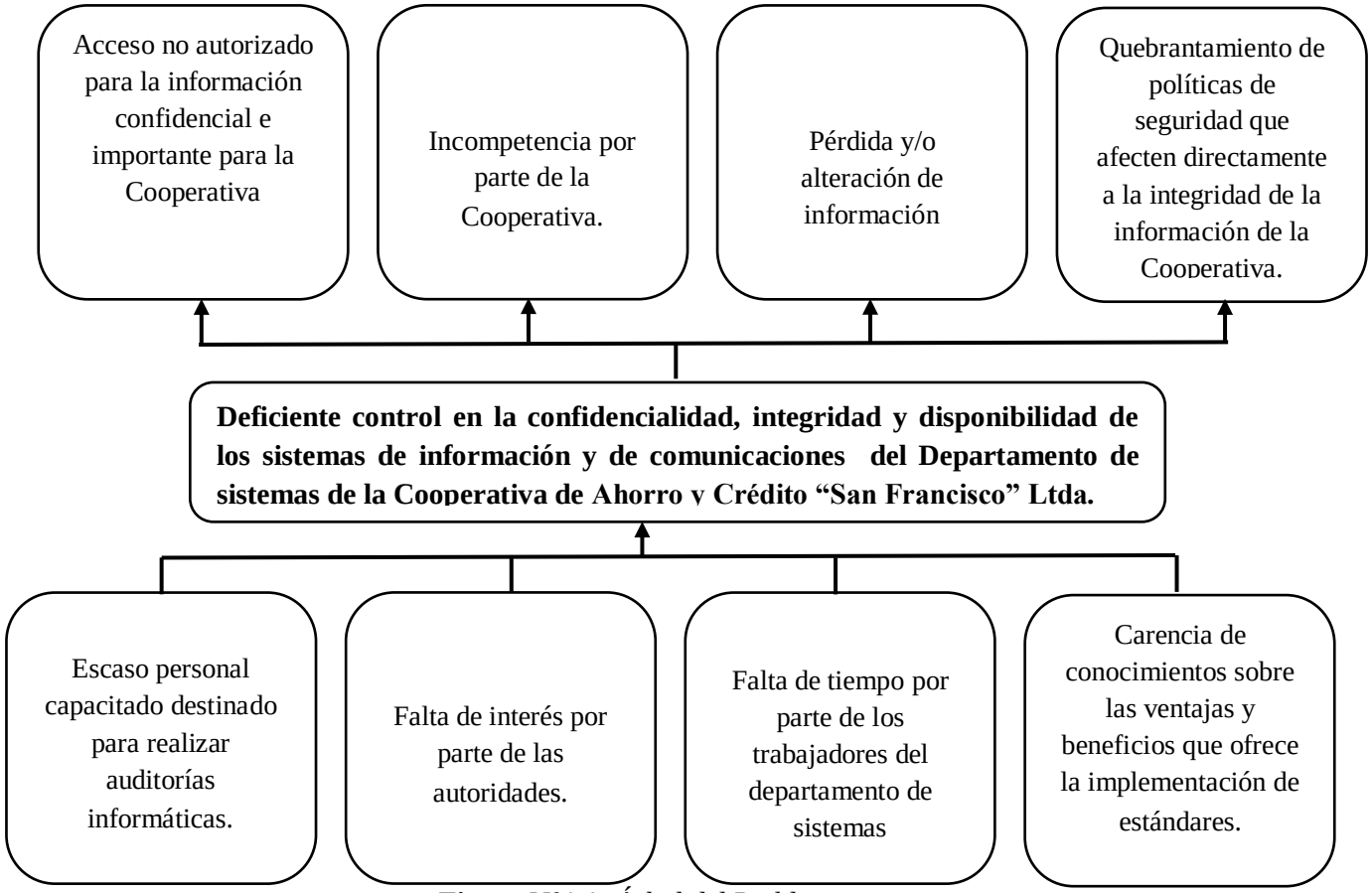

Figura N°1.1: Árbol del Problema
Elaborado por: *Tania Guachi*

1.2.1 Análisis Crítico

En el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda. no se ha implementado la norma de seguridad informática ISO 27001 para asegurar y mantener la confidencialidad, integridad y disponibilidad de sus sistema de información y de comunicación, esto se debe a que no existe personal capacitado para la actividad destinada lo que ocasionaría que la Cooperativa exponga la información de manera crítica consiguiendo pérdidas económicas a futuro, a más de esto se presenta un desconocimiento de las ventajas que ofrece la implementación de estándares como es de la ISO 27001 provocando que la Cooperativa sea muy vulnerable para diversos atacantes que quieran afectar con la integridad de la información de la misma ó directamente a sus recursos informáticos causando daños y perjuicios.

1.2.2 Prognosis

De continuar esta situación la Cooperativa se mantendría de forma tradicional y expuesta a tener pedidas económicas, robo o alteración de la información.

Durante el tiempo en que la Cooperativa no disponga de adecuados mecanismos de controles de seguridad sobre los sistemas de información y de comunicación se lograría que los atacantes violen fácilmente las políticas de seguridad afectando la integridad de la información de la Cooperativa y ocasionando desprestigio y no competitividad de la misma.

1.3 Formulación del Problema

¿Qué incidencia tiene la Implementación de la norma de seguridad informática ISO 27001 en la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.?

1.4 Preguntas Directrices

1.4.1 ¿Se aplican medidas de seguridad informática en el departamento de sistemas de la Cooperativa?

1.4.2 ¿En qué nivel de confiabilidad, integridad y disponibilidad se encuentran los sistemas de información y comunicación del departamento de sistemas de la Cooperativa?

1.4.3 ¿De qué manera se mejorara la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa?

1.5 Delimitación del Problema

El presente proyecto abarcara lo que corresponde a la Implantación de la norma de seguridad informática ISO 27001 para mantener la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación. Se lo realizara en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., abarcando un periodo de duración de seis meses dando inicio desde la fecha de aprobación del proyecto.

1.6 Justificación.

Hoy en día los sistemas de información y de comunicación están ocupando una amplia área en el sector empresarial, institucional entre otros, los mismos que requieren que la información que se maneja debe ser confidencial, además que se cuente con políticas de seguridad para acceder a la misma.

La realización de este trabajo de investigación es de gran importancia porque se puede vincular la teoría con la práctica, ya que gracias a esto se puede complementar el desarrollo de este proyecto y los resultados serán de gran ayuda en el desarrollo tecnológico logrando que la cooperativa cuente con normativas adecuadas y seguras sobre la protección de datos, privacidad y control de técnicas de información.

Una de las ventajas de la implantación de la norma de seguridad informática ISO 27001 es la reducción de gastos, generalmente se considera a la seguridad de la información como un costo sin una ganancia financiera evidente. Sin embargo, hay una ganancia financiera si se logra disminuir los gastos ocasionados por incidentes. Probablemente sí se produzcan dentro de la cooperativa interrupciones de servicio o esporádicos filtrados de datos, o tengan empleados descontentos, o ex empleados descontentos que afecten directamente a la integridad de la información de la misma.

La norma de seguridad informática ISO 27001 ayudará al ordenamiento del negocio por lo tanto obligará a definir de forma muy precisa tanto las responsabilidades como las obligaciones que hay que hacer y cumplir y, de esta forma, se ayudará a reforzar la organización interna.

El uso de estándares como de la ISO 27001 es y será adoptada por varias instituciones, organizaciones y empresas las cuales manejan sistemas de información y de comunicación lo cual permitirá mantener un buen rendimiento y eficacia en los mismos logrando seguridad en la información.

El proyecto se realizará ya que se cuenta con información para el desarrollo del mismo, que permitirá la implantación de la norma de seguridad informática ISO 27001 en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., permitiendo mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación.

1.7 Objetivos

1.7.1 Objetivo General

- Implantar la norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

1.7.2 Objetivos Específicos

- Investigar las normas y/o procesos de seguridad informática aplicadas en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.
- Analizar los parámetros de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.
- Implantar la norma de seguridad informática ISO 27001 para operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) del Departamento de Sistemas de la Cooperativa.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Revisado archivos investigativos desde de las fuentes bibliográficas de Internet se ha encontrado los siguientes trabajos:

"Implementación del primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, certificado bajo la norma ISO 27001:2005" elaborado por José Alfonso Aranda Segovia trabajo realizado en Guayaquil-Ecuador en el año 2009 en cuyas conclusiones dice lo siguiente:

La norma ISO 27001 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos; esto garantiza que ante recursos limitados las inversiones sean bien focalizadas, para lograr ello se necesita de la concientización de la compañía ya que es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Además al tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significa contar con seguridad máxima en la información de la organización sino que esto representa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

"Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, para la Intranet de la Corporación Metropolitana de Salud" elaborado por: Flor María Álvarez Zurita y Pamela Anabel García

Guzmán Segovia trabajo realizado en Quito-Ecuador en el año 2007 en cuyas conclusiones dice lo siguiente:

El Sistema de Gestión de Seguridad de la Información se define para cada organización en base a los riesgos que esté expuesta y los aspectos intrínsecos de su funcionamiento, y debe alinearse con la actividad de la organización; para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de Tecnologías de Información; una adecuada monitorización de los recursos de la red permite determinar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación; no se considera necesario extender el SGSI a toda la organización, lo primordial es centrarse en los procesos principales de la organización donde la parte de las actividades relacionadas con la gestión de la información, que suele coincidir con las áreas de sistemas de la información donde la seguridad de la información que se gestiona es crítico para las actividades del desarrollo del negocio. Mediante la planificación se logra una adecuada implementación del SGSI, en donde se analiza el negocio para determinar los activos más importantes, posteriormente se realiza un análisis de los riesgos que las amenazas y vulnerabilidades pueden generar, los cuales serán gestionados con controles apropiadamente implementados y criterios establecidos; asimismo para el establecimiento de seguridad de la información se considera tres pilares fundamentales: tecnología, procesos y las personas: Las empresas comúnmente invierten grandes sumas de dinero en tecnología y definición de procesos, y se han descuidado del personal de la empresa convirtiéndose así en el eslabón más débil de la cadena de seguridad, por esta razón es fundamental concienciar y fomentar la cultura de la seguridad de la información.

2.2 Fundamentación Legal

2.2.1 Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

TÍTULO PRELIMINAR

Artículo 1.- Objeto de la Ley .- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

TÍTULO I
DE LOS MENSAJES DE DATOS
CAPÍTULO I
PRINCIPIOS GENERALES

Artículo 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Artículo 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Artículo 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Artículo 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Artículo 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Artículo 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos. Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Artículo 8.- Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; éste requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

- Que la información que contenga sea accesible para su posterior consulta;
- Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
- Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
- Que se garantice su integridad por el tiempo que establezca en el Reglamento a esta Ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Artículo 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Artículo 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

- **Momento de emisión del mensaje de datos.-** Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto.

- **Momento de recepción del mensaje de datos.-** Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario.

Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,

- Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal

Artículo 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

- Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
- Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Artículo 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

- **Momento de emisión del mensaje de datos**.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto.
- **Momento de recepción del mensaje de datos.-** Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,
- **Lugares de envío y recepción.-** Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Artículo 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo. [Extraído desde http://sinar.gov.ec/downloads/L_comercio.pdf]

2.2.2 Ley de Propiedad Intelectual

TITULO PRELIMINAR

Art. 1.- El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las Decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador.

La propiedad intelectual comprende:

- Los derechos de autor y derechos conexos.

La propiedad industrial, que abarca, entre otros elementos, los siguientes:

- Las invenciones;
- Los dibujos y modelos industriales;
- Los esquemas de trazado (topografías) de circuitos integrados;
- La información no divulgada y los secretos comerciales e industriales;
- Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;
- Las apariencias distintivas de los negocios y establecimientos de comercio;
- Los nombres comerciales;
- Las indicaciones geográficas; e,
- Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

Las obtenciones vegetales.

Las normas de esta Ley no limitan ni obstaculizan los derechos consagrados por el Convenio de Diversidad Biológica, ni por las leyes dictadas por el Ecuador sobre la materia.

SECCIÓN I

PRECEPTOS GENERALES

Programa de ordenador (software): Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un dispositivo de lectura automatizada, ordenador, o aparato electrónico o similar con capacidad de procesar información, para la realización de una función o tarea, u obtención de un resultado determinado, cualquiera que fuere su forma de expresión o fijación. El programa de ordenador comprende también la documentación preparatoria, planes y diseños, la documentación técnica, y los manuales de uso.

Publicación: Producción de ejemplares puesto al alcance del público con el consentimiento del titular del respectivo derecho, siempre que la disponibilidad de tales ejemplares permita satisfacer las necesidades razonables del público, teniendo en cuenta la naturaleza de la obra.

SECCIÓN II

OBJETO DEL DERECHO DE AUTOR

Art. 8.- La protección del derecho de autor recae sobre todas las obras del ingenio, en el ámbito literario o artístico, cualquiera que sea su género, forma de expresión, mérito o finalidad. Los derechos reconocidos por el presente Título son independientes de la propiedad del objeto material en el cual está incorporada la obra y su goce o ejercicio no están supeditados al requisito del registro o al cumplimiento de cualquier otra formalidad.

SECCIÓN V

DISPOSICIONES ESPECIALES SOBRE CIERTAS OBRAS

PARÁGRAFO PRIMERO DE LOS PROGRAMAS DE ORDENADOR

Art. 28.- Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 29.- Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual.

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor.

Art. 30.- La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:

Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;

Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,

Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse.

Art. 31.- No se considerará que exista arrendamiento de un programa de ordenador cuando éste no sea el objeto esencial de dicho contrato. Se considerará que el programa es el objeto esencial cuando la funcionalidad del objeto materia del contrato, dependa directamente del programa de ordenador suministrado con dicho objeto; como cuando se arrienda un ordenador con programas de ordenador instalados previamente.

Art. 32.- Las excepciones al derecho de autor establecidas en los artículos 30 y 31 son las únicas aplicaciones respecto a los programas de ordenador.

Las normas contenidas en el presente Párrafo se interpretarán de manera que su aplicación no perjudique la normal explotación de la obra o los intereses legítimos del titular de los derechos. [Extraído desde http://www.cetid.abogados.ec/archivos/80.pdf]

2.3 Gráfica de inclusión de las Categorías Fundamentales

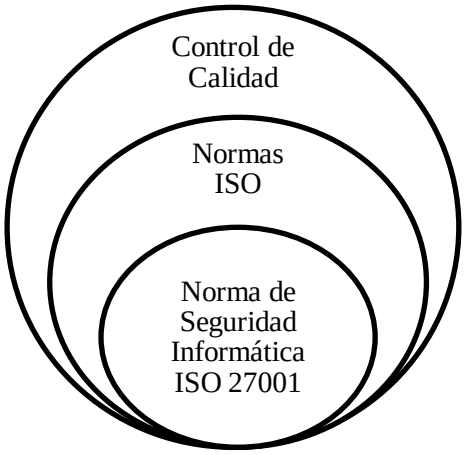

Figura N°2.1: Categoría Fundamental Variable Independiente
Elaborado por: *Tania Guachi*

Figura N°2.2: *Categoría Fundamental Variable Dependiente*
Elaborado por: *Tania Guachi*

2.3.1 Constelación de Ideas

Figura Nª. 2.3. *Constelación de ideas de la variable independiente*
Elaborado por: *Tania Guachi*

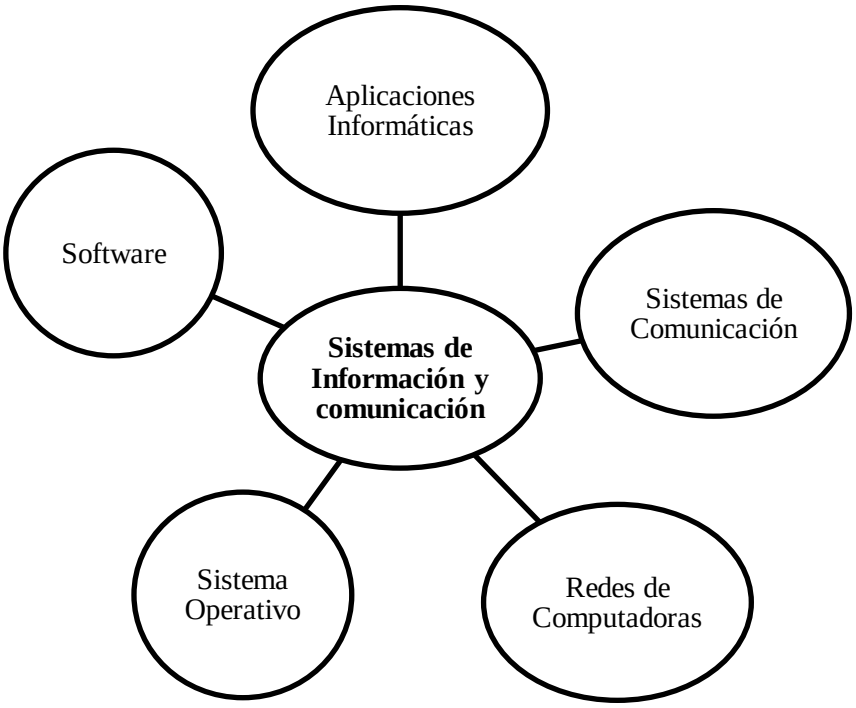

Figura Nª. 2.4. *Constelación de ideas de la variable dependiente*
Elaborado por: *Tania Guachi*

2.4 Categorías Fundamentales

2.4.1 Control de Calidad

Definición de Control de Calidad

Es el conjunto de técnicas y actividades de acción operativa que se utilizan, actualmente, para evaluar los requisitos que se deben cumplir con estándares respecto de la calidad del producto o servicio, cuya responsabilidad recae, específicamente, en el trabajador competente. Un factor importante para el funcionamiento de una organización es la calidad de sus productos y servicios. El proceso de control tiene la naturaleza de un ciclo de retroalimentación.

El control incluye la siguiente secuencia universal de pasos:

- Seleccionar el sujeto de control: esto es, escoger lo que se quiere regular.
- Elegir una unidad de medida.
- Establecer una meta para el sujeto de control.
- Crear un sensor que pueda medir el sujeto de control en términos de la unidad de medida.
- Medir el desempeño real.
- Interpretar la diferencia entre el desempeño real y la meta.
- Tomar medidas (si es necesario) sobre la diferencia.

La anterior secuencia de pasos es universal, es decir, se aplica al control de costos, al control de inventario, al control de calidad, etcétera.

El seguimiento detallado de los procesos dentro de una empresa para mejorar la calidad del producto y/o servicio se lo realiza mediante la implantación de

programas, mecanismo, herramientas y/o técnicas de la empresa para la mejora de la calidad de sus productos, servicios y productividad.

El control de la calidad es una estrategia para asegurar el cuidado y mejora continua en la calidad ofrecida consiguiendo cumplir los objetivos de la empresa.

Ventajas de establecer procesos de control de calidad

- Muestra el orden, la importancia y la interrelación de los distintos procesos de la empresa.
- Se realiza un seguimiento más detallado de las operaciones que se realizan dentro de la empresa.
- Se detectan los problemas antes y se corrigen más fácilmente de manera eficiente.

2.4.2 NORMAS ISO

Norma

Una norma es un modelo, un patrón, ejemplo o criterio a seguir que tiene por finalidad definir las características que deben poseer un objeto y los productos que proporcionan una compatibilidad con otros productos y así podrán ser usados a nivel internacional.

ISO

La ISO (International Standarization Organization) es una entidad internacional encargada de coordinar y unificar las normas nacionales, es decir ayuda a establecer la normalización en el mundo.

Definición de Norma ISO

Norma ISO se denomina a un conjunto de normas en las que se establecen los diferentes modelos de aseguramiento de calidad, facilitando así la

coordinación y unificación de las normas internacionales e incorporando la idea de estandarización logrando beneficios para los productores y compradores de bienes y servicios.

Las normas ISO surgieron en el año 1987 por la Organización Internacional de Normalización (International Standard Organization ISO), formada por más de 90 Organismos de Normalización, aparecieron como consecuencia de la internacionalización de los mercados, logrando la fortaleza de los mismos y la necesidad de incrementar la competitividad de productos y servicios.

Estructura de la organización.- La Organización ISO está compuesta por tres tipos de miembros:

- Miembros natos, uno por país, recayendo la representación en el organismo nacional más representativo.

- Miembros correspondientes, de los organismos de países en vías de desarrollo y que todavía no poseen un comité nacional de normalización. No toman parte activa en el proceso de normalización pero están puntualmente informados acerca de los trabajos que les interesen.

- Miembros suscritos, países con reducidas economías a los que se les exige el pago de tasas menores que a los correspondientes.

[Extraído desde http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_para_la_Estandarizaci%C3%B3n]

La familia ISO

Las series de normas ISO relacionadas con la calidad constituyen lo que se denomina familia de normas, las que abarcan distintos aspectos relacionados con la calidad:

- **ISO 9000:** Sistemas de Gestión de Calidad Fundamentos, vocabulario, requisitos, elementos del sistema de calidad, calidad en diseño, fabricación, inspección, instalación, venta, servicio post venta, directrices para la mejora del desempeño.

- **ISO 10000:** Guías para implementar Sistemas de Gestión de Calidad (SGC)/ Reportes Técnicos.- Guía para planes de calidad, para la gestión de proyectos, para la documentación de los SGC, para la gestión de efectos económicos de la calidad, para aplicación de técnicas estadísticas en las Normas ISO 9000. Requisitos de aseguramiento de la calidad para equipamiento de medición, aseguramiento de la medición.

- **ISO 14000:** Sistemas de Gestión Ambiental de las Organizaciones. Principios ambientales, etiquetado ambiental, ciclo de vida del producto, programas de revisión ambiental, auditorías.

- **ISO 19011:** Directrices para la Auditoría de los SGC y/o Ambiental

[Extraído desde http://www.unlu.edu.ar/~ope20156/normasiso.htm**]**

Importancia

Básicamente una norma ISO sirve como garantía de calidad, debido a la presión que ejerce el cliente sobre la necesidad de adquirir un producto de calidad. Su importancia radica en la confianza que se genera entre el proveedor, el producto y el cliente. Por otro lado sirve de ayuda para que una empresa, organización, cooperativa o entidad se vuelva competitiva, ya que si un tercero realiza una audición y comprueba que los productos y sistemas son buenos, pues los comprarán esto conllevará a tener beneficios dentro de la organización ya que incrementará la productividad.

2.4.3 Norma de seguridad informática ISO 27001

El estándar para la seguridad de la información ISO/IEC 27001 fue aprobado y publicado como estándar internacional en octubre de 2005 por International

Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

Los objetivos de seguridad pueden variar considerablemente dependiendo del sector en el que se encuentre la organización, pero de forma general estos objetivos están directamente ligados a la seguridad de procesos organizativos, procesos de producción, al ciclo de vida de la información y obviamente, al cumplimiento de la legislación vigente.

Figura N°2.4.1: *Aspectos que cubre la norma ISO 27001*
Fuente: *http://www.tcpsi.com/vermas/ISO_27001.htm*

La norma adopta una aproximación de proceso al establecimiento, a la implementación, a la operación, al monitoreo, a la revisión, al mantenimiento y a la mejora del Sistema de Gestión de Seguridad de la Información (SGSI) de una organización.

"BS 7799 es un estándar publicado originalmente por Grupo BSI en 1995. Fue escrito por el Reino Unido Departamento de Gobierno de Comercio e Industria (DTI), y consistió en varias partes.

La primera parte, que contiene las mejores prácticas para la Gestión de Seguridad de la Información, fue revisado en 1998, después de una larga

discusión en los organismos de normalización en todo el mundo, fue finalmente aprobado por la ISO como ISO / IEC 17799, "Tecnologías de la Información - Código de buenas prácticas para la gestión de seguridad de la información", en el año 2000. ISO / IEC 17799 fue revisado en junio de 2005 y, finalmente, incorporado en la serie ISO 27000 de normas como ISO / IEC 27002 en julio de 2007.

La segunda parte de BS 7799 se publicó por primera vez por BSI en 1999, conocida como BS 7799 parte 2, titulada "Información sobre Sistemas de Gestión de seguridad: Especificación con orientación para su uso" BS 7799-2 se centró en cómo implementar un sistema de gestión de seguridad de la información (SGSI), en referencia a la estructura de información de gestión de seguridad y los controles identificados en la BS 7799-2, que más tarde se convirtió en la norma ISO / IEC 27001. La versión 2002 de BS 7799-2 presentó el Plan-Do-Check-Act (PDCA) (modelo de aseguramiento de la calidad de Deming), alineándola con las normas de calidad como ISO 9000.

BS 7799 parte 2 fue adoptado por la ISO como ISO / IEC 27001 en noviembre de 2005.

BS7799 Parte 3 se publicó en 2005, que abarca el análisis de riesgos y la gestión. Se alinea con la norma ISO / IEC 27001”

[Extraído desde http://en.wikipedia.org/wiki/BS_7799]

La Organización Internacional de Estandarización (ISO) estableció la norma ISO 27001, la cual se emplea para la certificación. Ha reemplazado el estándar BS 7799 y brinda una norma internacional para sistemas de gestión de seguridad de la información. Con base en el estándar BS 7799, se la ha reorganizado para alinearse con otras normas internacionales. Se han incluido algunos nuevos controles, es decir, el énfasis en las métricas para la seguridad de la información y la gestión de incidentes.

Protegiendo activos

La norma plantea un enfoque completo a la seguridad de la información teniendo en cuenta que los activos que necesitan protección son: información digital, documentos en papel y activos físicos (computadoras y redes). Para lograr este objetivo se elabora mecanismos que van desde el desarrollo de competencia del personal de la organización hasta la protección técnica contra los fraudes informáticos.

ISO 27001 ayudará a proteger la información en términos de:

- Confidencialidad, que asegura la accesibilidad de la información solamente a los que estén autorizados a tener acceso.
- Integridad, que protege la precisión y la totalidad de la información y los métodos de procesamiento.
- Disponibilidad, que asegura que los usuarios autorizados tengan acceso a la información y activos relacionados cuando se lo exija.

En conformidad con otras normas de sistemas de gestión la norma ISO 27001 está alineada con otros sistemas de gestión y soporta la implementación y la operación coherente e integrada con normas de gestión relacionadas. El resultado es: Armonización con normas de sistemas de gestión como ISO 9001 e ISO 14001.

Además la norma ISO proporciona un énfasis en la mejora continua de procesos del SGSI.

Este estándar promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización, así también adopta el modelo de proceso Planear-hacer-chequear-actuar (PDCA), el cual se puede aplicar a todos los procesos del Sistema de Gestión de Seguridad de la Información.

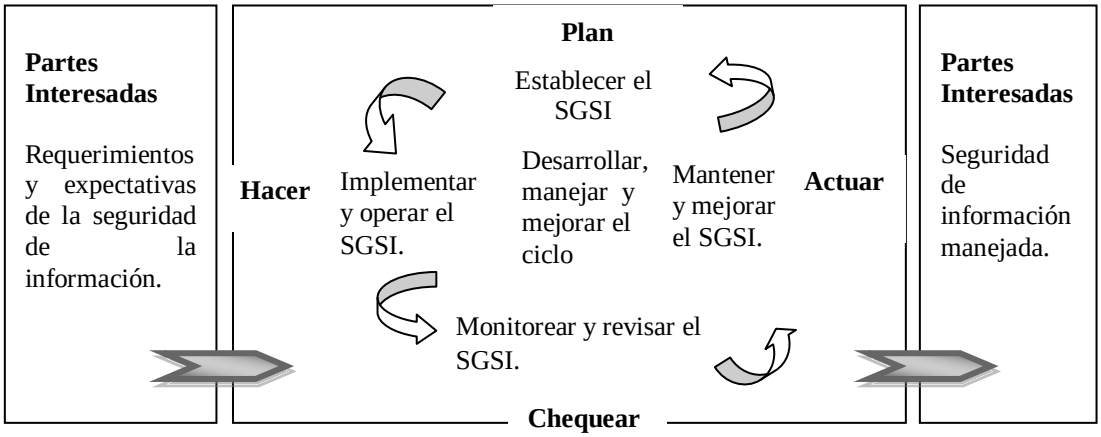

Figura N°2.4.2: *Modelo PDCA aplicado a los procesos SGSI*
Elaborado por: *Tania Guachi*

Beneficios

- Diferenciación sobre la competencia y el mercado.
- Mejora del conocimiento de los sistemas de información, sus problemas y los medios de protección.
- Protección de la información y cumplimiento legal sobre esta materia.
- Mejora la confianza de clientes y socios al aumentar las garantías de calidad, confidencialidad y disponibilidad.
- Reducción de costos (económicos y de imagen) vinculados a incidencias que afecten al tratamiento de la información.
- Acceso a oportunidades de negocio donde se valoren o incluso se exijan a los proveedores certificaciones reconocidas como por ejemplo con organismos gubernamentales y clientes de sectores específicos (banca, seguros, farmacéuticas, salud, aeroespacial, etc.).
- Establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.

- Los riesgos y sus respectivos controles son revisados constantemente.
- Las auditorías externas e internas permiten identificar posibles debilidades del sistema.
- Continuidad en las operaciones del negocio tras incidentes de gravedad.

2.4.4 Software

Software es una palabra proveniente del inglés (literalmente: partes blandas o suaves), que en nuestro idioma no posee una traducción adecuada al contexto, por lo cual se la utiliza asiduamente sin traducir. Se refiere al equipamiento lógico o soporte lógico de un computador digital, comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

Clasificación del software

Se puede clasificar al software de la siguiente forma:

Software de sistema: Es aquel que permite que el hardware funcione. Su objetivo es desvincular adecuadamente al programador de los detalles del computador en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc.

Software de programación: Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluye entre otros:

- Editores de texto
- Compiladores

- Intérpretes
- Enlazadores
- Depuradores

Software de aplicación: Aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios.

Sistema operativo

Un sistema operativo es un programa que controla la ejecución de los programas de aplicación y que actúa como interfaz entre las aplicaciones del usuario y el hardware de un computador. Se considera que un Sistema Operativo tiene tres objetivos:

- **Comodidad:** Un sistema operativo hace que un computador sea más cómodo de utilizar.
- **Eficiencia:** Un sistema operativo permite que los recursos de un sistema informático se aprovechen de manera más eficiente.
- **Capacidad de evolución:** Un sistema operativo debe construirse de modo que permita el desarrollo efectivo, le verificación y la introducción de nuevas funciones en el sistema y, a la vez, no interferir en los servicios que brindan,

Un sistema operativo desempeña funciones como:

Interfaces del usuario.- Es la parte del sistema operativo que permite comunicarse con él de tal manera que se puedan cargar programas, acceder archivos y realizar otras tareas. Existen tres tipos básicos de interfaces: las que se basan en comandos, las que utilizan menús y las interfaces gráficas de usuario**.**

Administración de recursos.- Sirven para administrar los recursos de hardware y de redes de un sistema informativo, como el CPU, memoria, dispositivos de almacenamiento secundario y periféricos de entrada y de salida.

Administración de archivos.- Un sistema de información contiene programas de administración de archivos que controlan la creación, borrado y acceso de archivos de datos y de programas. También implica mantener el registro de la ubicación física de los archivos en los discos magnéticos y en otros dispositivos de almacenamiento secundarios.

Administración de tareas.- Los programas de administración de tareas de un sistema operativo administran la realización de las tareas informáticas de los usuarios finales. Los programas controlan que áreas tiene acceso al CPU y por cuánto tiempo. Las funciones de administración de tareas pueden distribuir una parte específica del tiempo del CPU para una tarea en particular, e interrumpir al CPU en cualquier momento para sustituirla con una tarea de prioridad. [Extraído desde http://es.kioskea.net/contents/systemes/sysintro.php3]

2.4.5 Aplicaciones y Redes Informáticas

Aplicación informática

Es un programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.

Características de las aplicaciones informáticas

- En general, una aplicación es un programa compilado, escrito en cualquier lenguaje de programación.
- Las aplicaciones pueden tener distintas licencias de distribución como ser freeware, shareware, trialware, etc.

- Las aplicaciones tienen algún tipo de interfaz, que puede ser una interfaz de texto o una interfaz gráfica (o ambas).

Las aplicaciones informáticas suelen resultar una solución informática para la automatización de ciertas tareas complicadas como puede ser la contabilidad o la gestión de un almacén. Ciertas aplicaciones desarrolladas a medida suelen ofrecer una gran potencia ya que están exclusivamente diseñadas para resolver un problema específico. Otros, llamados paquetes integrados de software, ofrecen menos potencia pero a cambio incluyen varias aplicaciones, como un programa procesador de textos, de hoja de cálculo y de base de datos.

Redes Informáticas

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos (sistema de comunicación), que comparten información, recursos, servicios, etc. incrementando la eficiencia y productividad de las personas.

Estructura de las redes

a) El Software de Aplicaciones.- Conjunto de programas que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).

b) El software de Red.- Conjunto de programas que establecen protocolos para que los ordenadores se comuniquen entre sí. Dichos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

c) **El Hardware de Red.-** Esta formado por los componentes materiales que unen los ordenadores. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otros ordenadores.

Servicios de Redes

Servicios de Internet.- Los servicios de internet son productos de software que proporcionan los servicios tradicionales de internet a los clientes, en realidad la Web (por medio de los navegadores), FTP (Protocolo de transmisión de ficheros) y correo electrónico son todos los servicios que pueden ser tan útiles dentro de la red local como en internet, y muchos otros servicios dependiendo de las necesidades de los clientes.

Impresión en Red.- El aspecto más evidente es que compartir impresoras hace posible a dos o más usuarios imprimir trabajos al mismo tiempo. Una solución es la impresión en red debe incluir por consiguiente algún medio de almacenar los trabajos pendientes en una cola hasta que la impresora este libre para procesarlo cuando realiza este proceso de almacenar trabajos de impresión temporalmente en una unidad de disco, se dice que se ponen los trabajos en la cola de impresión.

Conexión a Internet.- El acceso a internet se ha convertido en una parte omnipresente de las redes de los equipos. Básicamente dar acceso a internet a los usuarios de una red consiste en establecer una conexión internet y compartirla en red destinada para las necesidades de los usuarios y de los servicios vitales para la empresa

Seguridad de Red.- La seguridad es esencial en cualquier red, y muchas de las tareas cotidianas de mantenimiento de la administración de red que se llevan a cabo están relacionadas con la seguridad proporcionada por los diversos componentes de la red y los datos del sistema de daños accidentales o

del acceso no autorizado. El objetivo del proceso de administración de seguridad es proporcionar a los usuarios accesos a todos los recursos que necesitan, mientras se les asila de aquellos que no necesitan. El uso adecuado de las herramientas de administración de seguridad proporcionadas por los componentes de la red es esencial para mantener una red segura y productiva.

2.4.6 Sistemas de Información y Comunicación

Sistemas de información

Una organización es un sistema. Sus componentes (mercadotecnia, manufactura, ventas, investigación, embarques contabilidad y personal) trabajan juntos para crear utilidades que beneficien tanto a los empleados como a los accionistas de la compañía. Todo sistema organizacional depende en medida, de una entidad abstracta denominada *sistema de información.* Este sistema es el medio por el cual los datos fluyen de una persona o departamento hacia otros y pueden ser cualquier cosa, desde la comunicación interna entre los diferentes componentes de la organización y líneas telefónicas hasta sistemas de cómputo que generan reportes periódicos para varios usuarios. Los sistemas de información proporcionan servicios a todos los demás sistemas de una organización y enlazan todos sus componentes en forma tal que estos trabajen con eficiencia para alcanzar el mismo objetivo.

Los sistemas de información están formados por subsistemas que incluyen hardware, software, medios de almacenamiento de datos para archivos de base de datos. El conjunto particular de subsistemas utilizados (equipo específico, programas, archivos y procedimientos) se les denomina una aplicación de sistemas de información. De esta forma, los sistemas de información pueden tener aplicaciones en ventas, contabilidad o compras. Además un sistema de información es un conjunto de componentes interrelacionados que permiten reunir, procesar, almacena y distribuir información para apoyar la toma de decisiones y el control de una organización.

Así mismo los sistemas de información también ayudan a los administradores y trabajadores:

- a analizar problemas,
- visualizar aspectos complejos,
- crear productos nuevos.

Un sistema de información produce la información que las organizaciones necesitan para:

- tomar decisiones,
- controlar operaciones,
- analizar problemas,
- crear y producir y/o servicios nuevos.

Las actividades de un sistema de información son: entrada, procesamiento y salida. La entrada captura o recolecta datos del interior de la organización o de su entorno para ser procesados en un sistema de información. El procesamiento convierte las entradas brutas en una forma que tiene más sentido para los humanos. La salida transfiera la información procesada a las personas que la usarán o las actividades en las que será usada. Los sistemas de información también requieren retroalimentación que consiste en salidas que se devuelven a los miembros apropiados de la organización para ayudarles a evaluar o corregir la etapa de entrada.

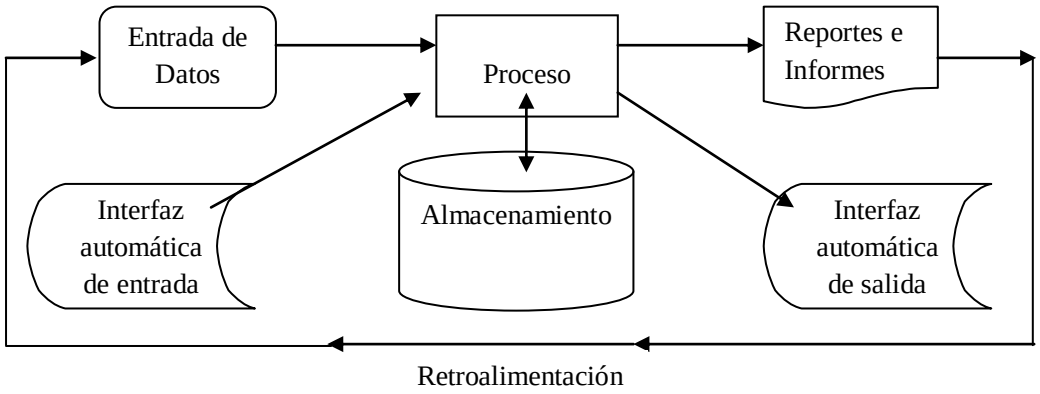

Figura N°2.4.3: *Ciclo de un Sistema de Información*
Elaborado por: *Tania Guachi*

Tipos y Usos de los Sistemas de Información

Los sistemas de información dentro de las organizaciones cumplen los siguientes objetivos:

- Automatización de procesos operativos.
- Proporcionar información que sirva de apoyo al proceso de toma de decisiones.
- Lograr ventajas competitivas a través de su implantación y uso.

a) **Sistemas Transaccionales.**

Son el primer sistema de Información que se implementa en la empresa. Inicia apoyando las tareas a nivel operativo de la organización para continuar con los mandos intermedios y posteriormente la alta administración, conforme evolucionan.

Función: Procesa transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc.

b) **Sistemas de Apoyo de las Decisiones.**

Se define a este sistema, como un conjunto de programas y herramientas que permiten realizar el análisis de las diferentes variables de negocio con la finalidad de apoyar el proceso de toma de decisiones.

Función: Ayuda a la toma de decisiones de los administradores al combinar datos, modelos analíticos sofisticados y software amigable en un solo sistema poderoso que puede dar soporte a la toma de decisiones de la organización.

c) **Sistema de Información estratégico**

Puede ser considerado como el uso de la tecnología de la información para soportar o dar forma a la estrategia competitiva de la organización, a su plan para incrementar o mantener la ventaja competitiva o bien reducir la ventaja de sus rivales.

Función: No brinda apoyo a la automatización de los procesos operativos ni proporciona información para apoyar a la toma de decisiones. Sin embargo, este tipo de sistemas puede llevar a cabo dichas funciones. [Extraído desde http://luisa-silva.lacoctelera.net/post/2008/04/22/informatica-principios-los-sistema-informacion]

Sistemas de Comunicación

Comunicación.- Transferencia de información de un lugar a otro lugar y que debe ser: eficiente, confiable, segura.

Definición: Componentes o subsistemas que permiten la transferencia/ intercambio de información.

En la siguiente figura se muestra un diagrama a bloques del modelo básico de un sistema de comunicaciones, en éste se muestran los principales componentes que permiten la comunicación.

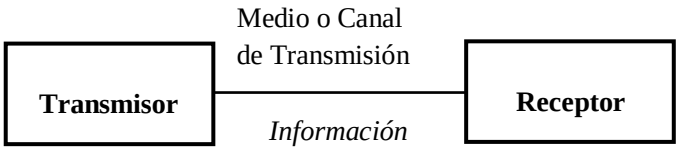

Figura N°2.4.4: *Modelo básico de un sistema de comunicaciones*
Elaborado por: *Tania Guachi*

Elementos básicos de un sistema de comunicaciones

En toda comunicación existen tres elementos básicos (imprescindibles uno del otro) que son:

a) **Transductor de entrada.-**Convierte el mensaje a un formato adecuado para su trasmisión.

   El Transmisor pasa el mensaje al canal en forma de señal. Para lograr una transmisión eficiente y efectiva, se deben desarrollar varias operaciones de procesamiento de la señal. La más común e importante es la modulación, un proceso que se distingue por el acoplamiento de la señal transmitida a las propiedades del canal, por medio de una onda portadora, otra operación que existe también es la codificación que elimina redundancia presente en el mensaje (compresión) y se agrega redundancia (bits de paridad) para aumentar inmunidad frente al ruido. (JPEG).

b) **Canal de Transmisión.-** o medio es el enlace eléctrico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio puede ser un par de alambres, un cable coaxial, el aire, etc. Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, la disminución progresiva de la potencia de la señal conforme aumenta la distancia.

   La función del Receptor es extraer del canal la señal deseada y entregarla al transductor de salida. Como las señales son frecuentemente muy débiles, como resultado de la atenuación, el receptor debe tener varias etapas de amplificación. En todo caso, la operación clave que ejecuta el receptor es

la demodulación, el caso inverso del proceso de modulación del transmisor, con lo cual vuelve la señal a su forma original.

c) **Transductor de salida.-** Convierte la señal eléctrica a su entrada en una forma de onda adecuada

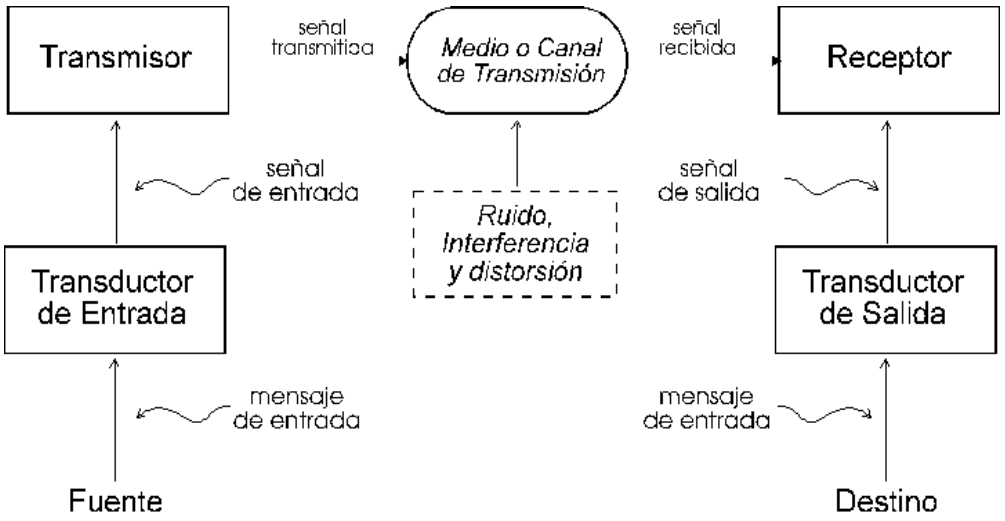

Figura N°2.4.5: *Elementos de un sistema de comunicación*
Fuente: *http://www.eveliux.com/mx/modelo-de-un-sistema-de-comunicaciones.php*

Características deseables de un Sistema de Comunicación

- Buena fidelidad
- Potencia de señal baja
- Trasmitir una gran cantidad de información
- Ocupar un ancho de banda pequeño
- Bajo costo (complejidad)
- Las operaciones digitales complejas se han hecho mucho más baratas

2.5 Hipótesis

La implantación de la norma de seguridad informática ISO 27001 mejorará la confianza en el manejo de los sistemas de información y comunicación del departamento de sistemas de la cooperativa.

2.6 Determinación de Variables

Variable independiente

Norma de seguridad informática ISO 27001.

Variable dependiente

Sistemas de información y comunicación.

CAPITULO III

METODOLOGÍA

3.1 Enfoque

El enfoque de la investigación se realizó de forma cualitativa ya que se obtuvo información directa de los investigados por medio de la aplicación de una entrevista, gracias a esto se pudo elaborar un análisis de resultados y proponer alternativas de solución.

3.2 Modalidad básica de la investigación.

3.2.1 Investigación Bibliográfica – Documental

Se realizó una investigación bibliográfica acudiendo a libros, tesis, monografías e incluso al recurso más importante como es el internet para obtener información más profunda con respecto a problemas similares, de esta manera se recopiló información valiosa que fue usada como sustento científico del proyecto.

3.2.2 Investigación de Campo

Mediante la elaboración de este tipo de investigación se tuvo la oportunidad de estar cerca y conocer el entorno donde se desenvuelve el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "SAN FRANCISCO" Ltda., accediendo a la posibilidad de tener el contacto directo entre el investigador y la realidad, obteniendo información de acuerdo a los objetivos planteados inicialmente.

3.3 Nivel o tipo de Investigación

3.3.1 Exploratorio

Se realizó una investigación de nivel exploratorio, para determinar las condiciones actuales de la seguridad de los sistemas de información y de comunicación.

3.3.2 Descriptivo

El proceso investigativo tuvo un nivel descriptivo para conocer con profundidad el problema, estableciendo sus causas y consecuencias así como las dificultades por lo que está atravesando.

3.3.3 Asociación de variables

Se determinó la relación de una variable con la otra y la incidencia que tiene en la solución del problema.

3.4 Población y muestra

3.4.1 Población

El proyecto está orientado a una población integrada por cinco personas que laboran en el departamento de sistemas de la Cooperativa de Ahorro y Crédito "SAN FRANCISCO" Ltda.

3.4.2 Muestra

La muestra pasaría a ser la misma población puesto que ésta es muy reducida.

3.5 Recolección de información

3.5.1 Plan de Recolección de Información

Las personas que proporcionarán la información serán: Administrador de redes, Jefe del departamento de Sistemas, dos Desarrolladores y el Asistente de Mantenimiento.

Para recabar la información se utilizará técnicas como la observación y la entrevista con sus respectivos instrumentos que son el registro de datos y un cuestionario de entrevistas

3.5.2 Procesamiento y análisis de la Información

3.5.2.1 Procesamiento y análisis de la información (Plan que se empleará para procesar la información recogida.)

Lo primero que se realizará al recopilar la información, será seleccionar los datos que se requiere para el desarrollo del proyecto los mismos que será analizados en relación con el problema y para poder establecer las conclusiones respectivas asegurando que los datos sean lo más reales posibles.

3.5.2.2 Plan de análisis e interpretación de resultados

El análisis de los resultados se realizará desde el punto de vista descriptivo y estadístico, proceso que permite realizar la interpretación adecuada basada en el marco teórico, relacionado las variables de la investigación y la propuesta lo que servirá para establecer las conclusiones y recomendaciones.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de la necesidad

La Cooperativa de Ahorro y Crédito "San Francisco" Ltda., al ser una institución prestigiosa de la ciudad de Ambato brinda servicios eficaces a la ciudadanía ya que cuenta con el Departamento de Sistemas que da soporte a los sistemas de información , comunicación y a los usuarios.

El Departamento de Sistemas de la Cooperativa en busca de mejoras para los sistemas de información y comunicación opta por ayudar a estudiantes egresados de la Carrera de Ingeniería en Sistemas para que realicen proyecto de trabajo de graduación y de esta manera mejorar y optimizar las tareas que realizan a diario así también elevar el nivel de desempeño de la Cooperativa.

4.2 Análisis de Resultados

La investigación se realizó mediante la aplicación de entrevistas al personal que labora en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

MATRIZ RESULTADOS DE LA ENTREVISTA

Entrevistado / Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Se aplican políticas de seguridad para la información? Si….. Enúncielas; No…. Porqué?	Existen políticas definidas así: • Como usuarios con sus respectivas contraseñas para poder acceder a la computadora y a los sistemas de información • Perfil de acceso de uso para los usuarios • Política para el uso de internet y de correo electrónico.	Si, como por ejemplo: • Autorizaciones de Gerencia y de Administración • Autorización de recursos humanos (encargado de crear los roles y usuarios dependiendo de las funciones que desempeña) • Identificación del personal	Si: • Roles y acceso de usuarios. • Prioridad de usuarios. • Horarios de acceso.	Pues tenemos: • Creación de usuarios y roles dependiendo de las funciones. • El acceso a los servidores es restringido. • Restricciones del uso de flash memory	Contamos con: • Respaldos • Antivirus • Copias de Seguridad
¿De qué manera se realiza un control de la seguridad de la información?	Se realiza con: • Auditorías externas mediante un auditor informático que realiza estas tareas. Se cuenta con manuales de monitoreo para los jefes departamentales.	Se controla: Mediante módulos: Módulos de administración/seguridad/ usuarios/páginas/roles. Las páginas se relacionan con roles y los roles con los usuarios.	• Se asigna roles y controles de acuerdo a funciones de cada empleado Se cuenta con una bitácora de cambios de las funciones y desempeño de los empleados que registra el departamento de Recursos Humanos.	Mediante el uso de roles de cada usuario.	Mediante el uso de Check point, Firewall, IPTable de LINUX.

Entrevistado / Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Describa el control interno informático que se realiza en el Departamento de Sistemas?	El control se realiza: • Por el envió de respaldos de custodia externa (archivos logs) • Bitácora de visitas a sitios de internet • Control Biométrico • Custodio de claves para los sistemas.	En cuanto a Redes se hace mediante una red local y red inalámbrica, la red inalámbrica se gestiona con un AccesPoint y Chek Point. El acceso a la información es mediante contraseñas	Es "buena" ya que se maneja por contraseñas de acceso, subredes, la seguridad se define como una pequeña o mediana empresa.	Se basa en usuarios con sus respectivo roles y de igual forma el acceso a los sistemas de información es a base de contraseñas.	Controlando permanente con reglas de seguridad, actualizando a diario los servidores de antivirus.
¿Conoce usted acerca de un Sistema de Gestión de seguridad de la información (SGSI)?	Si, tales como: • Sistemas de encriptación de discos PGP • Active Directory • Sistemas de Password de una sola vez	No, la verdad solo de active directory nada mas	No, Pero conozco : • LDAP Microsoft (Active Directory) • OPENLDAP • Es un Control más granulad para acceder a la información • Tiene un nivel de seguridad elevado	No, tal vez conozca con otro nombre pero no escuchado de un sistemas de gestión de seguridad de la información	Como el Check Point ya que por medio de este no se puede ingresar a páginas inseguras, ni los usuarios externos pueden ingresar a páginas institucionales. También es por el uso de IP TABLES

Entrevistado / Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?	• Encriptación de claves de acceso. • Enlaces de comunicación encriptados • Políticas de acceso restringido al uso de flash memory • Asignación de permisos por usuarios y perfiles • Gestión de claves custodiadas por alto nivel.	Se usa un servidor firewall con políticas establecidas por el mismo.	• Firewall de Check Point • Antivirus Anti Spam, Mallware anti hackers • Kaspersky Internet Security	• Check Point para seguridades • Software de Antivirus • Equipo de Linux en el que se realiza filtrado de URL	Roles y usuarios dependiendo de las funciones de cada usuario.
¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?	Si: • Mediante una unidad interna que se basa en la norma de BASILEA que asigna quienes van a ser designados para esta tarea. • Se realiza tareas de riesgos a base de eventos y de mejoras continuas	Si: Mediante la replicación de Base de Datos con tecnología RAID5	Si: Mediante un departamento de riesgos externo a este.	Si: Mediante un registro de los eventos sucedidos que informan los usuarios al departamento.	Dentro del sistema existe una página administración de riesgos puesto en vigilo por el administrador.

Entrevistado / Pregunta	Jefe de sistemas	Desarrollador 1	Desarrollador 2	Administrador de Sistemas	Asistente de mantenimiento
¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?	Si: • En los enlaces de comunicación • Trafico de red • Desempeño de servidores.	Si se lo realiza mediante la aplicación MRTG	Se lo realiza mediante sistemas que notifican cuando hay ataques	Básicamente se realiza por la revisión de logs. Los sistemas de comunicación cuentan con una aplicación web que informa los enlaces principales, además la aplicación MRTG.	Si: Se realiza todos los días para tener la conectividad con todas las oficinas y para reducir un margen de error de la conectividad.
¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación. Si…. De qué manera se lo ha realizado; No….. Porque?	Si: • Mediante un plan de contingencia • Simulacro de pérdida de enlace de datos • Pruebas de pérdida de energía eléctrica • Daños en los servidores de Base de Datos y de Aplicativos.	Se lo realiza mediante la utilización de un servidores de respaldos de Base de Datos	Si ha hecho uno cortando los sistemas de red esto se ha realizado junto con el auditor informático y el departamento de riesgos	Si se lo realiza ya que se dispone de un plan de contingencia del área.	Si he escuchado de eso, que lo han realizado pero no he participado en ese simulacro

Tabla Nº 4.1: *Matriz de resultado de la entrevista*
Elaborado por: *Tania Guachi*

4.3 Tabulación de los resultados

1. **¿Se aplican políticas de seguridad para la información? Si… Enúncielas; No…. Por qué?**

   Objetivo: Determinar si se aplican políticas de seguridad para la información

RESPUESTA	CANTIDAD	PORCENTAJE
Políticas para los usuarios	4	80%
No	0	0%
Políticas para los sistemas de información	1	20%
Políticas para los sistemas de comunicación	0	0%
Total	5	100%

Tabla Nº 4.2: *Cuadro porcentual Pregunta 1*
Elaborado por: *Tania Guachi*

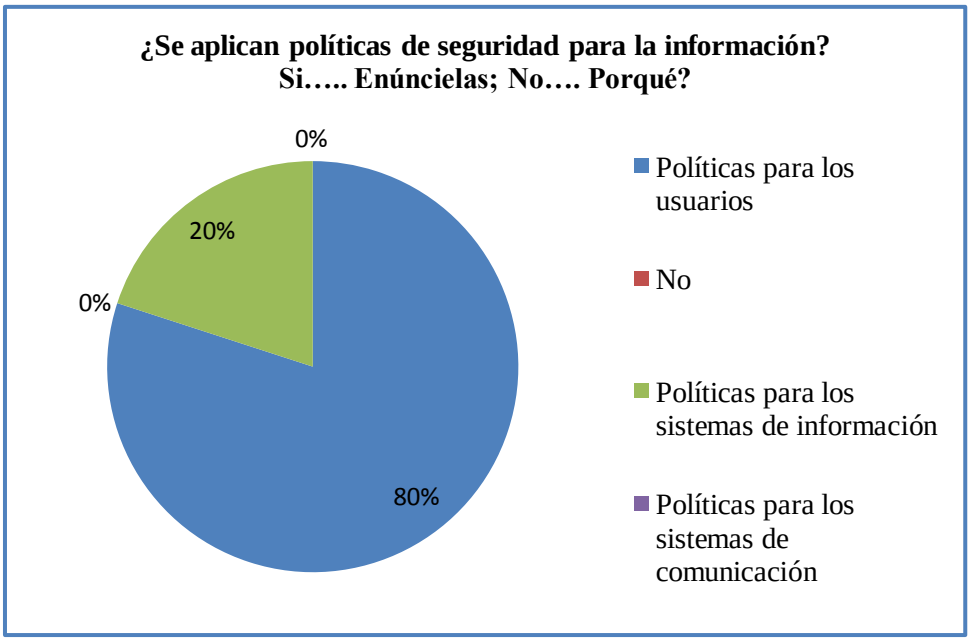

Figura Nº 4.1: *Gráfico Pregunta 1*
Elaborado por: *Tania Guachi*

Interpretación.- El 80% de los trabajadores respondieron que existen políticas establecidas solo para los usuarios, es decir cada uno es dueño de una contraseña para poder usar la computadora y las aplicaciones que utilicen, el 20% respondieron que se aplican políticas para los sistemas de información como respaldos, copias de seguridad y antivirus.

Análisis.- Solo se cuenta con políticas de seguridad destinadas para los usuarios, por lo que los sistemas de información y de comunicación están desprotegidos.

2. **¿De qué manera se realiza un control de la seguridad de la información?**
   Objetivo: Conocer si se realiza un control de seguridad de la información

RESPUESTA	CANTIDAD	PORCENTAJE
Auditoría externa	1	20%
Módulos de administración	2	40%
Bitácoras de cambios	1	20%
Mediante uso de aplicaciones	1	20%
Total	5	100%

Tabla Nº 4.3: *Cuadro porcentual Pregunta 2*
Elaborado por: *Tania Guachi*

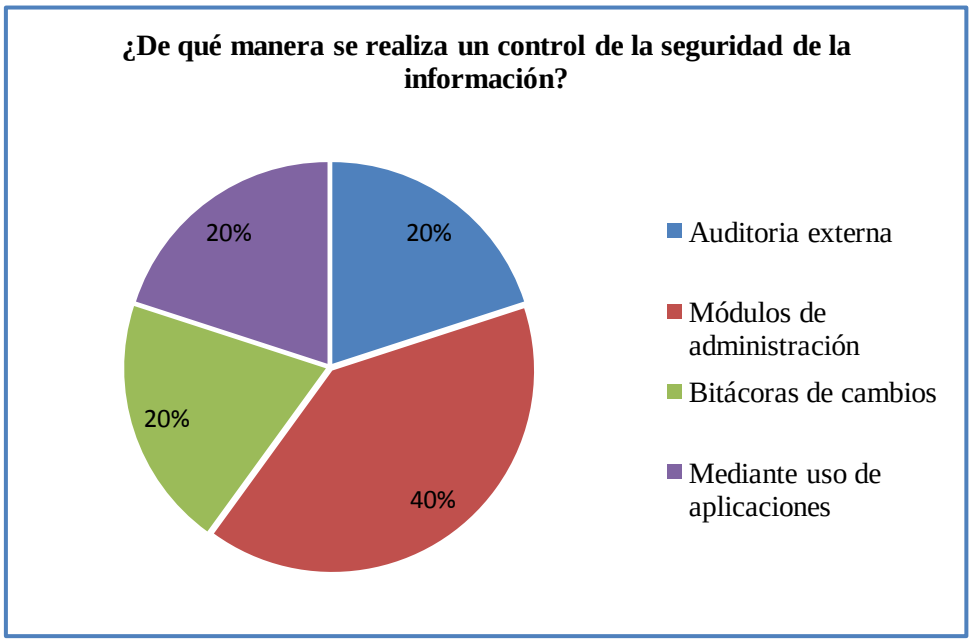

Figura Nº 4.2: *Gráfico Pregunta 2*
Elaborado por: *Tania Guachi*

Interpretación.- El 40% del personal entrevistado ha indicado que el control de seguridad de la información que realizan es mediante módulos de administración, en base a los perfiles de usuario, un 20% respondieron que se controla la seguridad de la información por medio de auditoría externa, la misma que es realizada por auditores informáticos externos al departamento de sistemas, otro 20% manifiesta que se lleva una bitácora de cambios de las funciones y desempeño de los empleados, finalmente el 20% respondió que se controla la seguridad de la información por el uso de aplicaciones como Check Point, Firewall.

Análisis.- No existe un control de seguridad para la información establecida por alguna herramienta destinada para llevar a cabo esta tarea.

3. **¿Describa el control interno informático que se realiza en el Departamento de Sistemas?**

Objetivo: Determinar si se realiza un control informático en el departamento de sistemas

RESPUESTA	CANTIDAD	PORCENTAJE
Buena	1	20%
Asignación de contraseñas	3	60%
Envió de respaldos	1	20%
Total	5	100%

Tabla Nº 4.4: *Cuadro porcentual Pregunta 3*
Elaborado por: *Tania Guachi*

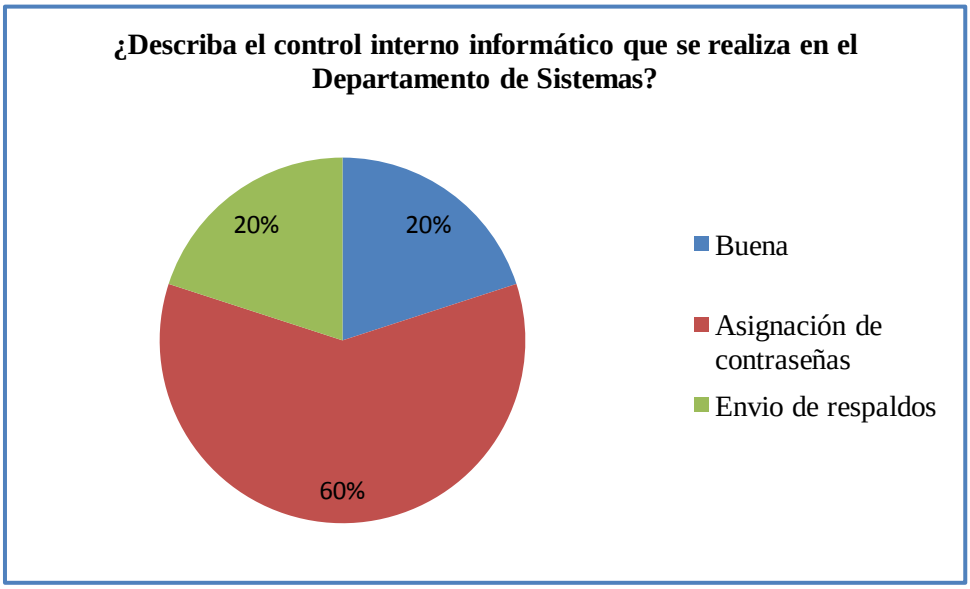

Figura Nº 4.3: *Gráfico Pregunta 3*
Elaborado por: *Tania Guachi*

Interpretación.- Según el gráfico se puede observar que el 60% de los entrevistados respondieron que se mantiene un control interno informático mediante asignación de contraseñas a los diversos usuarios de las aplicaciones informáticas, un 20% califico como buena al control informático ya que se lo trataba como una pequeña o mediana empresa al departamento de sistemas, por

último el 20% restante respondieron que se lo realiza por medio de envió de respaldos de custodia externa de los archivos log.

Análisis.- No se elabora un control a profundidad de todas las actividades relacionadas con los sistemas de información y de comunicación.

4. **¿Conoce usted acerca de un Sistema de Gestión de Seguridad de la Información (SGSI)?**

Objetivo.- Conocer si el personal que labora en el departamento de sistemas posee conocimientos acerca de un Sistema de Gestión de Seguridad de la Información.

RESPUESTA	CANTIDAD	PORCENTAJE
Si	1	20%
No	4	80%
Total	5	100%

Tabla Nº 4.5: *Cuadro porcentual Pregunta 4*
Elaborado por: *Tania Guachi*

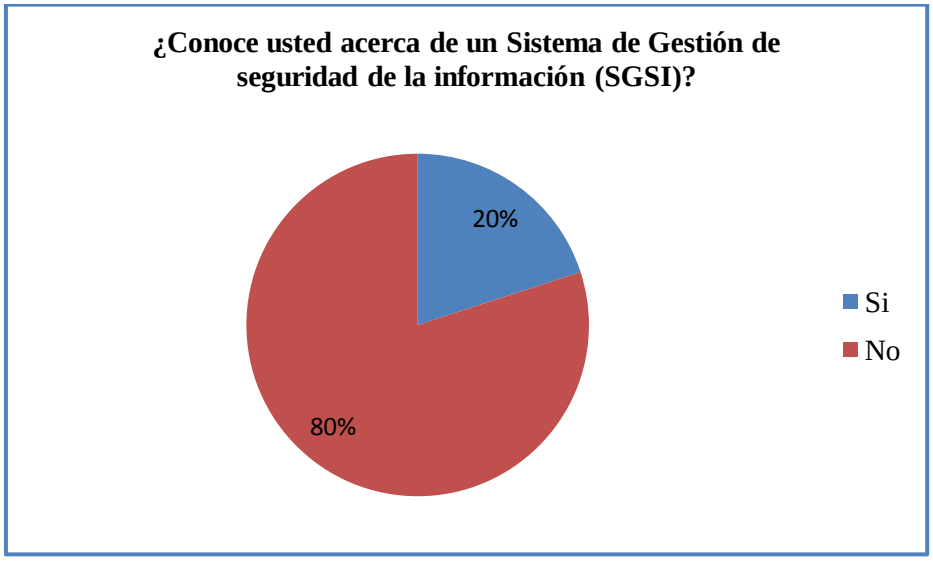

Figura Nº 4.4: *Gráfico Pregunta 4*
Elaborado por: *Tania Guachi*

Interpretación.- El 20% de las respuestas obtenidas describen que si conocen lo que realiza un sistema de gestión de seguridad de la información entre estas mencionan aplicaciones como sistemas de encriptación de discos PGP, Active Directory, y el 80 % restante indico que desconocen del tema.

Análisis.- En el departamento de sistemas casi en su totalidad no existe conocimiento de lo que es sistema de gestión de seguridad de la información, por lo tanto también desconocen las ventajas y beneficios que ofrece el contar con sistema como tal.

5. **¿Cómo se garantiza la confiabilidad, integridad y disponibilidad de la información que se procesa en los sistemas de información y de comunicación?**

Objetivo.- Conocer como se garantiza confiabilidad, integridad y disponibilidad de la información que se procesa en los sistemas de información y de comunicación

Respuesta.- La confiabilidad, integridad y disponibilidad de la información que se procesa en los sistemas de información y de comunicación se puede garantizar por el uso de sistemas de hardware y software robustos, por el uso de aplicaciones como Firewall, antivirus, por la realización de respaldos de la base de dato, además se cuenta con niveles de acceso definidos por perfiles es decir por el uso de contraseñas.

Análisis.- La confiabilidad, integridad y disponibilidad de la información se garantiza en base a los aspectos de hardware y software más no establecidos por normas o metodologías que permitan realizar esta tarea de manera más óptima.

6. **¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?**

   Objetivo.-Conocer si disponen de mecanismos, técnicas y/o herramientas de seguridad aplicadas para la seguridad de los sistemas de información y de comunicación.

   Respuesta.- Se usan mecanismo como encriptación de contraseñas, enlaces de comunicación encriptados, técnicas como gestión de claves custodiadas por alto nivel y herramientas como Check Point y Antivirus.

   Análisis.-Los mecanismos, técnicas y/o herramientas que son aplicadas para la seguridad de los sistemas de información y de comunicación brindan cierta parte seguridad a la información.

7. **¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?**

   Objetivo.-Conocer si se realizan tareas de control y administración de riesgos en el departamento de sistemas.

   Resultados.-Se realiza control de riesgos mediante un departamento de riesgos externo a este departamento en base a eventos de riesgos y mejora continua

   Análisis- El control de y administración de riesgos que se lleva a cabo no es de forma óptima ya que se lo realiza externamente

8. **¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?**

   Objetivo.- Conocer si se realizan tareas de monitoreo a los sistemas de información y de comunicación.

RESPUESTA	CANTIDAD	PORCENTAJE
Para los sistemas de información	1	20%
Para los sistemas de comunicación	4	80%
Total	5	100%

Tabla Nº 4.6: *Cuadro porcentual Pregunta 8*
Elaborado por: *Tania Guachi*

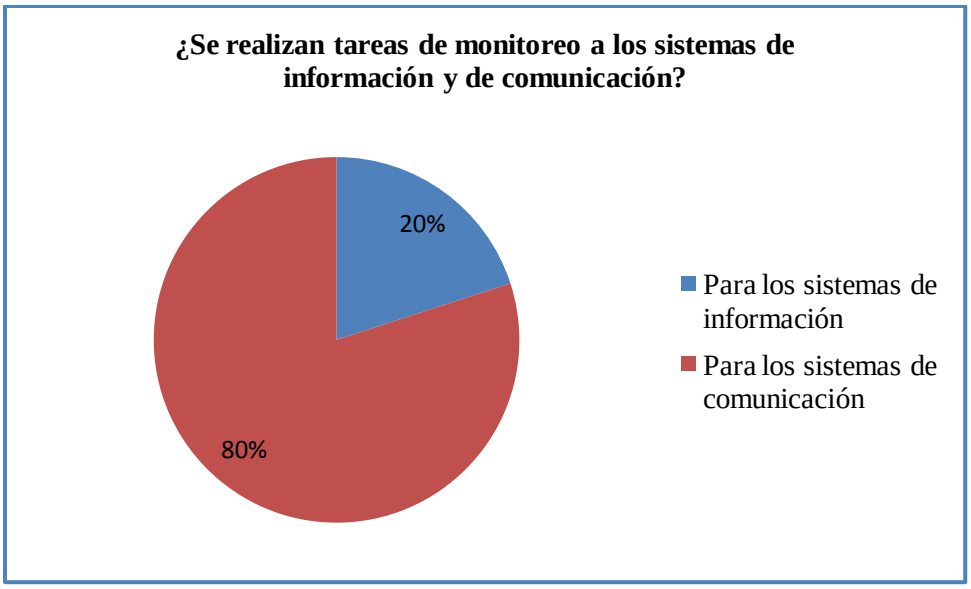

Figura Nº 4.5: *Gráfico Pregunta 8*
Elaborado por: *Tania Guachi*

Interpretación.-De la figura se puede deducir que el 80% indica que se realiza monitoreo a los sistemas de información y un 20% respondió que se efectúa tareas de monitoreo a los sistemas de comunicación.

Análisis.-Se realiza monitoreo a los sistemas de comunicación pero solo para verificar la conectividad y en los sistemas de información se hace por medio de la revisión de archivos log pero no es un tarea que se lo realiza planificada, por lo que están propensos a ser atacado.

9. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación. Si…. De qué manera se lo ha realizado; No….. Porqué?

Objetivo.-Conocer si se realizan simulacros frente a la caída de los sistemas de información y de comunicación

Respuesta.-Se ha realizado simulacros como pérdida de enlace de datos, pruebas de pérdida de energía eléctrica, daños en los servidores de Base de Datos y de Aplicativos.

Análisis.-Se ha realizado reducidos simulacros de la caída de los sistemas de información y de comunicación base a planes de contingencia que han sido escritos con anterioridad.

4.3 Interpretación de Resultados

Los trabajadores del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., proporcionaron información mediante una entrevista personal en lo cual se obtuvo lo siguiente:

- No existen políticas de seguridad establecidas para los datos e información.
- Desconocimiento de lo que es un Sistema de Gestión de Seguridad de la Información.
- No se utiliza metodologías para garantizar la confiabilidad, integridad y disponibilidad de la información.
- El control y administración de riesgos de la información no son realizados en base a técnicas por lo que se realiza externamente a este departamento.
- Falta definición de controles de seguridad informática para los sistemas de información y de comunicación.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La información que se procesa en los sistemas de información y de comunicación, no se encuentra protegida con metodologías.
- Los sistemas de información y de comunicación se encuentran expuestos a los ataques informáticos.
- En el departamento no existe una función que administre y controle los riesgos informáticos.
- No se cuenta con estándares de seguridad informática que ayuden a preservar las propiedades de confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación.

5.2 RECOMENDACIONES

- Se recomienda adoptar una metodología para mantener y mejorar la seguridad de la información.
- Es recomendable disponer de un control de todas las actividades relacionadas a los sistemas de información y de comunicación.
- Se recomienda auditar de manera permanente los sistemas de información y de comunicación.
- Es recomendable disponer de una arquitectura que unifique todos los mecanismos de seguridad informática.
- Se recomienda la implantación de la norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación.

CAPITUO VI

PROPUESTA

6.1. Tema

"Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda."

6.2. Datos Informativos

Institución: Cooperativa de Ahorro y Crédito "San Francisco" Ltda."

Ciudad: Ambato

Dirección: Montalvo y 12 de Noviembre

Investigador: Tania Verónica Guachi Aucapiña

Tutor: Ing. David Guevara

6.3. Antecedentes

Toda entidad, institución, empresa y organización poseen y operan con el principal activo que es la información, la misma que es procesada mediante el uso de sistemas de información y de comunicación, de esta manera se logra brindar un mejor servicio ya que se cuenta con medios automatizados.

Así la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., es una entidad cuya misión es ofrecer servicios financieros ejecutados con calidad, para contribuir al bienestar de los socios, clientes y la sociedad, la misma cuenta con un departamento de

sistemas que es el encargado de administrar los sistemas de información y de comunicación.

En el departamento de sistemas los trabajadores son conscientes de que la información que se almacena y se procesa mediante los sistemas de información y de comunicación es muy vital para el desempeño organizacional por lo que se debería contar con metodologías eficientes y óptimas de seguridad informática, ya que en este tiempo existen muchos hackers, personas e incluso sistemas hack que roban y/o alteran la información.

La implantación de la norma de seguridad informática ISO 27001 surge de la necesidad de contar con una metodología de calidad para la seguridad de la información con el objetivo de mejorar la confidencialidad, integridad y disponibilidad sistemas de información y de comunicación.

6.4. Justificación

La información en una entidad financiera como es la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., debe ser confiable, integra, segura y a disposición de los usuarios, la misma está expuesta a ser alterada o infringida por lo que se debería contar con mecanismos de seguridad informática.

En el departamento de sistemas no se encuentra implementada estándares o metodologías de seguridad de la información ya que los sistemas de información y de comunicación no se encuentran totalmente protegidos, por tal motivo se ha considerado implantar la norma de seguridad ISO 27001 que engloba en uno solo muchas técnicas de seguridad para la información.

La presente propuesta se la puede realizar porque se cuenta con facilidades necesarias para obtener información, se cuenta con el apoyo del departamento de sistemas y con herramientas necesarias para empezar con las actividades previstas.

6.5. Objetivos

6.5.1 Objetivo General

- Implantar la norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.

6.5.2 Objetivos Específicos

- Determinar el alcance para la aplicación del estándar ISO 27001 en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.

- Diseñar un Sistema de Gestión de Seguridad de la Información para mantener y mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación.

- Implantar la norma de seguridad informática ISO 27001 en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.

6.6. Análisis de factibilidad

6.6.1. Factibilidad Operativa

Para cumplir el objetivo, se implantará la norma de seguridad informática ISO 27001 con el apoyo de todos los trabajadores del departamento de sistemas y con la aprobación del Gerente de la Cooperativa. Se construirá un documento en donde describirá los pasos que se realizaran construyendo una metodología que garantice el cumplimiento de la norma de seguridad informática ISO 27001.

6.6.2. Factibilidad Económica

El proyecto es factible de realizarse debido a que se va a implantar en base al contenido descrito en la norma, seleccionando los aspectos de la ISO 27001 encajando a los sistemas de información y de comunicación de la Cooperativa.

Los trabajadores del departamento de sistemas, están interesados en el desarrollo del proyecto de tesis, ya que la implantación de la norma de seguridad de la información generará ahorros para la institución, por que los gastos serán sustentados por el desarrollador del proyecto de tesis.

6.6.3 Factibilidad Técnica

Para la implantación de la norma de seguridad informática ISO 27001 en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda. Se cuenta con la siguiente documentación:

- ISO 27001
- ISO27001-norma-e-implantacion-SGSI
- ISO/IEC 27002

6.7 Fundamentación

6.7.1 Introducción

En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo tanto es necesario que toda organización que busca excelencia en los servicios o productos que ofrece, adopte un Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. Para cubrir estas necesidades la ISO (Organización Internacional para la Estandarización) creó una norma que permite a las organizaciones encaminarse en un Sistema de Gestión de Seguridad de la Información, el cual es la ISO 27001:2005.

6.7.2 ¿Qué es la Norma ISO 27001:2005?.

Es la normativa para los Sistemas de Gestión de Seguridad de la Información, la cual evolucionó del estándar ISO 17799 que a su vez se derivó de la BS 7799. La finalidad de esta norma es permitir de forma sistemática minimizar el riesgo y proteger la información en las empresas.

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

La metodología de los sistemas de gestión se basa en el Ciclo de Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, cuyas pasos son: Planear, Implantar, Revisar y Mejorar o PLAN-DOCHECK- ACT (PDCA). La representación gráfica del ciclo de Deming abstrae el concepto de mejora continua por la retroalimentación del paso final al paso inicial.

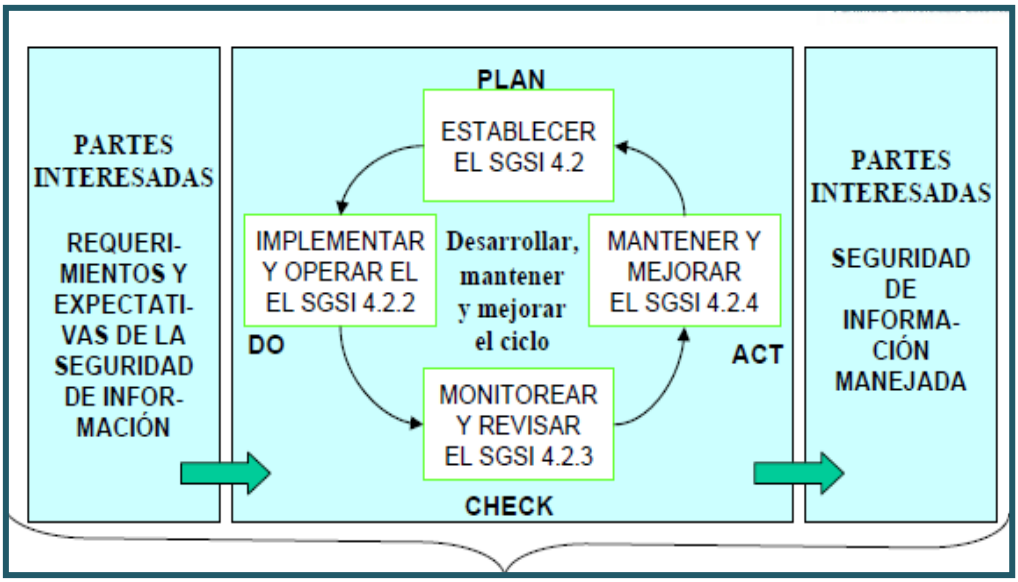

Figura Nº 6.1*. Clausulas de la Norma ISO 27001 distribuidas en Ciclo de Deming.*
Fuente: *http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf*

Planear (establecer el SGSI).- Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

Hacer (implementar y operar el SGSI) .- Implementar y operar la política, controles, procesos y procedimientos SGSI.

Chequear (monitorear y revisar el SGSI).-Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

Actuar (mantener y mejorar el SGSI).- Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

6.7.3 Contenido de la Norma

Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

6.7.3.1 Alcance

6.7.3.1.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

6.7.3.1.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza.

6.7.3.2 Referencias normativas

Los siguientes documentos mencionados son indispensables para la aplicación de este documento. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento citado.

ISO/IEC 17799:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

6.7.3.3 Sistema de gestión de seguridad de la información

6.7.3.3.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan.

Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA.

6.7.3.3.2 Modelo Plan-Do-Check-Act (PDCA)

El modelo PDCA obedece a un ciclo continuo que comienza en la fase de planificación y termina en la fase de implantar mejoras a raíz de los resultados de las métricas, auditorías internas etc. Toda esta actividad a su vez, retroalimenta la fase de planificación de un nuevo ciclo.

Figura Nº 6.2: *Modelo ISO 27001*
Fuente: *http://www.isoauditores.es/empieza-el-trabajo/como-se-implanta-iso-27001.html*

6.8 Metodología de implementación.

6.8.1 Establecer y manejar el SGSI

6.8.1.1 Establecer el SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de la justificación de cualquier exclusión del alcance.

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto.

b) Definir la política de seguridad:

- La política de seguridad establecerá el marco general y los objetivos de seguridad de la información de la organización.
- Tendrá en cuenta los requerimientos legales y contractuales relativos a la seguridad de la información.
- Estará alineada con el contexto estratégico de gestión del riesgo, será proporcionada y coherente.
- Establecerá los criterios de evaluación del riesgo.
- Estará aprobada por la dirección.

c) Definir el enfoque de valuación del riesgo de la organización

- Definir una **metodología de evaluación del riesgo** apropiada para el SGSI y los requerimientos de la actividad. Es esencial que los resultados de esta metodología sean comparables y reproducibles.

  Metodología de análisis y evaluación de riesgos.- La recomendación es usar un método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con facilidad. La metodología dada consiste que para cada activo se debe identificar todas las amenazas existentes, la posibilidad de ocurrencia de estas amenazas, las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la posibilidad que dicha amenaza penetre tal vulnerabilidad. El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la de posibilidad de amenaza.

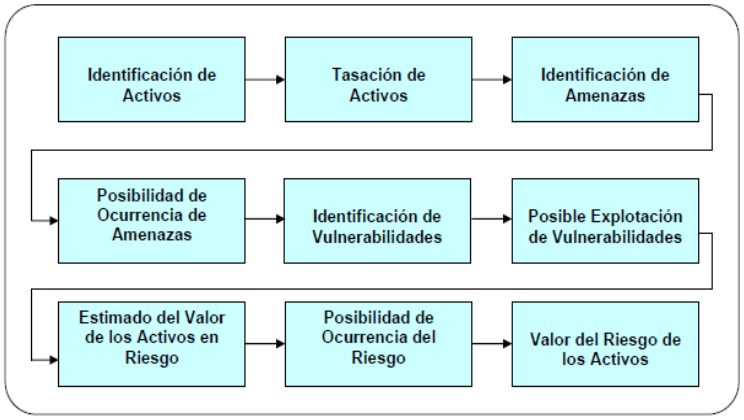

Figura Nº 6.3: *Metodología para el Análisis y Evaluación de Riesgos*
Fuente*: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf*

d) Identificar riesgos.

1. Identificación y tasación de activos.

Identificación de los activos de información:

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información. Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

El siguiente paso es tasar el listado de los activos para quedarnos con aquellos de valor. La pregunta para evaluar es **¿la pérdida o deterioro de este activo, cómo afecta la disponibilidad, confidencialidad e integridad del proceso**

del negocio de la compañía? , en nuestro caso se usará la escala de 1 a 5, siendo el 1 de menor afectación y 5 de afectación. El valor total del activo es el promedio entero de los valores asignados a la disponibilidad, confidencialidad e integridad.

Una vez calculado el valor por cada activo seleccionamos aquellos de valor, el valor umbral queda a discreción de cada organización por ejemplo serán de importancia aquellos con un valor mayor o igual a 3.

2. **Identificar amenazas y vulnerabilidades**: todas las que afectan a los activos establecidos en el área de estudio.

3. **Identificar los impactos**: Los sucesos o acciones que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

4. **Análisis y evaluación de los riesgos:** Para realizar estas acciones correctamente se debe:

    - Evaluar el impacto en el negocio que podría resultar de un fallo de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
    - Evaluar la posibilidad realista de que se produzca el fallo de seguridad en función de las amenazas y vulnerabilidades, los impactos asociados con estos activos, y los controles actualmente implantados.
    - Estimar los Niveles de riesgo.
    - Determinar si el riesgo es aceptable o requiere tratamiento usando los criterios de aceptación de riesgos establecidos.

e) Analizar y evaluar el riesgo

- Evaluar el impacto en la organización de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.
- Evaluar de forma realista la probabilidad de que ocurra un fallo de seguridad en relación a las amenazas, vulnerabilidades e impacto en los activos y los controles ya implementados.
- Estimar el nivel de riesgo.

f) Identificar y evaluar las distintas opciones de tratamiento de riesgo para:

- Aplicar los controles adecuados
- Aceptar el riesgo si esa aceptación cumple con la política y los criterios establecidos.
- Transferir el riesgo a terceros.

g) Seleccionar los objetivos de control y controles del Anexo A de la norma ISO 27001 para el tratamiento del riesgo que cumplan con los requisitos identificados en el proceso de evaluación y tratamiento del riesgo.

NOTA: El Anexo A contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones. Se dirige a los usuarios de este Estándar Internacional como un punto de inicio para la selección de controles para asegurar que no se pase por alto ninguna opción de control importante.

h) Definir el Statement of Applicability (SOA) (Declaración de aplicabilidad) que incluya:

- Los objetivos de control y controles seleccionados y los motivos de su selección
- Los objetivos de control y controles que actualmente están implantados
- Los objetivos de control y controles que han sido excluidos y los motivos de su exclusión.

NOTA: El Enunciado de Aplicabilidad proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo. El justificar las exclusiones proporciona un chequeo para asegurar que ningún control haya sido omitido inadvertidamente.

6.8.2 Implementar y operar el SGSI

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados.

c) Implementar los controles seleccionados en 6.8.1.1 (g) para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles.

e) Implementar los programas de capacitación y conocimiento.

f) Manejar recursos para el SGSI.

g) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad.

6.8.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:

   1. Detectar prontamente los errores en los resultados de procesamiento;

2. identificar prontamente los incidentes y violaciones de seguridad fallida y exitosa;
3. ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y
4. determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

6.8.4 Mantener y mejorar el SGSI

Se debe realizar regularmente lo siguiente:

- Implementar las mejoras identificadas en el SGSI.
- Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.
- Asegurar que las mejoras logren sus objetivos señalados.

6.9 MODELO OPERATIVO

6.9.1 Desarrollo de la implantación

6.9.1.1 Establecer y manejar el SGSI

a) Alcance

"La provisión de un sistema de gestión de seguridad de información, para los procesos de: Gestión de software antivirus, Desarrollo de Sistemas, Mantenimiento de Equipos y Administración del Sistema en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda.".

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto. El alcance para el Departamento de Sistemas está destinado hacia los servicios de:

- Desarrollo de sistemas informáticos
- Mantenimiento preventivo de hardware y software de la institución.
- Monitoreo de redes y servicios de terceros
- Centralización de la emisión de estructuras de información a los organismos de control
- Gestión del correo electrónico.
- Brindar seguridades a nivel de firewall y acceso a los equipos de cómputo
- Administración del software antivirus

Así también el departamento de sistemas brinda el apoyo y soporte a los usuarios de los sistemas de información.

b) Política

La política de seguridad definida para la implantación del Sistema de Gestión de Seguridad de la Información es:

"Proveer Servicios de Calidad con un Sistema de Gestión de Seguridad de la Información basado en la Prevención y enfocado a minimizar el riesgo de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación " .

- **Objetivos**

  Para dar cumplimiento a la política establecida se ha definido objetivos.

Objetivo General:

- Implementar un sistema de gestión de seguridad de la información

Objetivos Específicos:

- Establecer medidas de seguridad para evitar las violaciones de seguridad
- Establecer un mecanismo de control de riesgos de la información
- Implementar un sistema de gestión de seguridad de la información

c) Enfoque de valuación del riesgo en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

La metodología adoptada para la estimación de riesgo es la siguiente

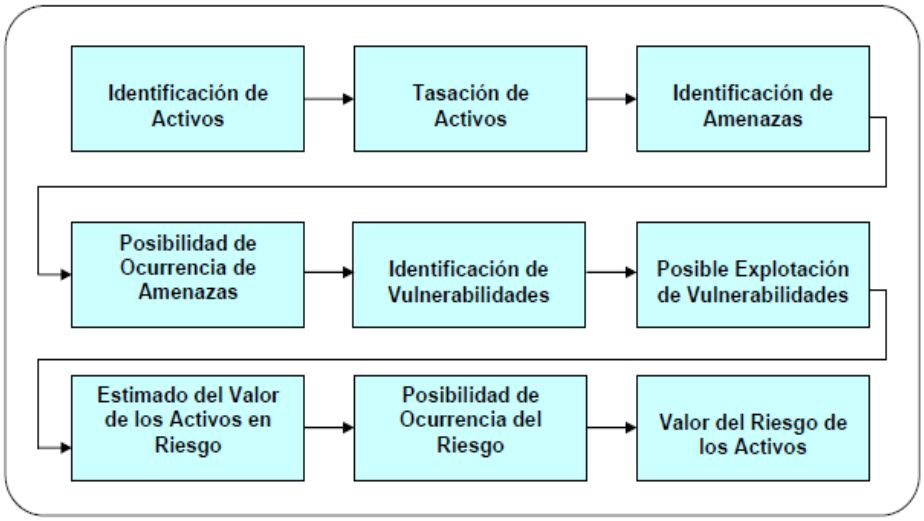

Figura Nº 6.4: *Metodología para el Análisis y Evaluación de Riesgos*
Fuente*: http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf*

d) Identificación de los riesgos

1. Identificación y tasación de activos.

Activos con sus respectivos valores de confidencialidad, disponibilidad e integridad que han sido identificados en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Computadores de Oficina	2	4	2	3
Computadores portátiles	1	1	2	1
Switch	2	4	3	3
Hubs	1	1	2	1
Impresoras	2	4	2	3
Router	3	4	3	3
Servidor usado para servicios Web: Cajeros Móviles Web Service de interfaz a buró de crédito	2	4	2	3
Bridge	5	5	4	5
Servidor que aloja el sistema y la base de datos del Software de Prevención de lavado de Activos	3	4	2	3
Servidor sistema de Administración de Talento Humano por Competencias Compers Software de Riesgo de Liquidez y Mercado	2	3	2	2
Scanner	2	1	2	2
Servidor de Base de Datos Sistema Sifiz y servidor de contingencias de sistema Sifiz	3	4	3	3
Servidor de aplicaciones Sifiz institucional (Core financiero) y servidor de contingencias de BD institucional	4	5	4	4
Servidor que aloja los blades de software Check Point de : Firewall IPS IDS VPN	5	4	5	5

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de interface servicios de terceros con el Banco del Austro: Cajeros Automáticos Tarjetas de débito Chequeras	4	3	4	4
Servidor que alojará el controlador de dominio institucional	3	3	3	3
Servidor de contingencias de BD y aplicaciones ubicado en la oficina Salcedo	3	4	3	3
Software para cajero automático	2	4	3	3
Software cuentas corrientes	3	4	3	3
Sistema financiero sifiz	3	4	3	3
Programa interface ahorros , tarjetas y cuentas corrientes	3	4	3	3
Extreme software para el manejo de la interface de tarjetas de crédito(Servidor coopsanfra)	2	1	1	1
Software kaspersky enterprise spaces licencia (80)	2	1	3	2
Software check point security bundle(firewall)	3	4	2	3
Equipos tape backup 100 gb para respaldar información	3	4	2	3
Ups	2	4	2	3

Tabla Nº 6.1: *Activos del departamento de sistemas*
Elaborado por: *Tania Guachi*

De la tabla anterior se selecciona a los activos cuyo valor total es igual o mayor a 3, para hacer uso de estos para el análisis y evaluación de riesgos.

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Computadores de Oficina	2	4	2	3
Switch	2	4	3	3
Impresoras	2	4	2	3
Router	3	4	3	3
Servidor usado para servicios Web: Cajeros Móviles Web service de interfaz a buró de crédito	2	4	2	3
Bridge	5	5	4	5
Servidor que aloja el sistema y la base de datos del Software de Prevención de lavado de Activos	3	4	2	3
Servidor sistema de Administración de Talento Humano por Competencias Compers Software de Riesgo de Liquidez y Mercado	2	3	2	2
Scanner	2	1	2	2
Servidor de Base de Datos Sistema Sifiz y servidor de contingencias de sistema Sifiz	3	4	3	3
Servidor de aplicaciones Sifiz institucional (Core financiero) y servidor de contingencias de BD institucional	4	5	4	4

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor que aloja los blades de software Check Point de : Firewall IPS IDS VPN	5	4	5	5
Servidor de interface servicios de terceros con el Banco del Austro: Cajeros Automáticos Tarjetas de débito Chequeras	4	3	4	4
Servidor que alojará el controlador de dominio institucional	3	3	3	3
Servidor de contingencias de BD y aplicaciones ubicado en la oficina Salcedo	3	4	3	3
Software para cajero automático	2	4	3	3
Software cuentas corrientes	3	4	3	3
Sistema financiero sifiz	3	4	3	3
Programa interface ahorros , tarjetas y cuentas corrientes	3	4	3	3
Extreme software para el manejo de la interface de tarjetas de crédito(Servidor coopsanfra)	2	1	1	1
Software kaspersky enterprise spaces licencia (80)	2	1	3	2
Software check point security bundle(firewall)	3	4	2	3
Equipos tape backup 100 gb para respaldar información	3	4	2	3
Ups	2	4	2	3

Tabla Nº 6.2: *Activos importantes del departamento de sistemas*
Elaborado por: *Tania Guachi*

e) Analizar y evaluar el riesgo

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Computadores de Oficina	A Virus	4	A1 Falta de mantenimiento	4	3	4	12
			A2 Falta de controles de acceso	3			
	B Spyware	3	B1 Abuso del internet	3			
			B2 Falta de control de acceso	3			
	C Phishing	2	C1 Falta de herramientas de monitoreo	3			
	D Malware	3	D1 Abuso del Internet	3			
Switch	A Recalentamiento	3	A1 Falta de mantenimiento.	4	3	3	9
			A2 Flujo de energía.	4			
Impresoras	A Cartucho de impresión dañados.	4	A1 Falta de mantenimiento	4	3	4	12
	B. Papel atascado	3	B1 Exceso de impresiones	3			

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Router	A Virus	4	A1 Falta de mantenimiento	4	3	4	12
			A2 Falta de instalación de programas de monitoreo	4			
	B Rendimiento	3	B1 Mucho tráfico del internet	4			
Servidor usado para servicios Web: Cajeros Móviles Web service de interfaz a buró de crédito	A Robo de información	4	A1 Falta de monitoreo	4	3	4	12
	B Desfiguración de la página web	4	B1 Falta de mantenimiento	3			
Bridge	A Ineficiencia	3	A1 Grandes interconexiones de redes	3	5	3	15
			A2 saturación de las redes por tráfico de difusión	3			
Servidor que aloja el sistema y la base de datos del Software de Prevención de lavado de Activos	A Alteración y/o pérdida de los datos.	4	A1 Escasas medidas de seguridad	4	3	4	12
			A2 Imposición de restricciones	4			

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Servidor de Base de Datos Sistema Sifiz y servidor de contingencias de sistema Sifiz	A Alteración y/o pérdida de los datos	4	A1 Escasas medidas de seguridad	4	3	4	12
			A2 Imposición de restricciones	4			
Servidor de aplicaciones Sifiz institucional (Core financiero) y servidor de contingencias de BD institucional	A Alteración y/o pérdida de los datos	4	A1 Escaso medidas de seguridad	4	4	4	16
	B Mal funcionamiento del sistema	4	B1 Falta de mantenimiento	3			
			B2 Mal uso por parte de los usuarios	4			
Servidor que aloja los blades de software Check Point de : Firewall IPS IDS VPN	A Ineficiencia	3	A1 Mala administración	3	5	4	20
	B Alteración y/o pérdida de los datos	4	B1 Escaso de medidas de seguridad.	4			
Servidor de interface servicios de terceros con el Banco del Austro: Cajeros Automáticos Tarjetas de débito Chequeras	A Sin servicio	4	A1 Falla de conexión	4	4	4	16
	B Ineficiencia	3	B1 Mala administración	4			

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Servidor que alojará el controlador de dominio institucional	A Error en autentificación de los usuarios	4	A1 Infracción en el manejo de controlador del dominio institucional	3	3	4	12
			A2 Escaso de políticas de seguridad	4			
Servidor de contingencias de BD y aplicaciones ubicado en la oficina Salcedo	A Desactualización	4	A1 Falta de actualización de datos y de información	4	3	4	12
Software para cajero automático	A Inseguridad	4	A1 Falta de mecanismos de seguridad	4	3	4	12
	B Sin servicio	3	B1 Acceso no autorizado	3			
			B2 Manipulación errónea del sistema	3			
			B3 Falta de mantenimiento	4			
Software cuentas corrientes	A Datos erróneos	3	A1 Alteración de los datos	3	3	3	9

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Sistema financiero sifiz	A Intercepción e Interrupción	4	A1 Falta de planes de contingencia	3	3	4	12
	B Modificación	3	B2 Falta de mantenimiento	3			
			B2 Falta de herramientas de seguridad	4			
Programa interface ahorros , tarjetas y cuentas corrientes	A Sin servicio	3	A1 Falta de mantenimiento	3	3	3	9
Software check point security bundle(firewall)	A Ineficiencia	4	A1 Mal Uso	3	3	4	12
			A2 Mala configuración	4			
			A3 Mala administración	4			
	B Fallas en el software	4	B1Falta de mantenimiento	3			
Equipos tape backup 100 gb para respaldar información	A Daños físicos	4	A1 Mal funcionamiento	3	3	4	12
			A2 Mal uso	3			
			A3 Método erróneo de almacenamiento del dispositivo	3			
	B Escases de Cintas	3	B1Desatención	3			

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo
Ups	A Contaminantes peligrosos suspendidos en el aire	3	A1 Situaciones de riesgo para el personal y/o falta de confiabilidad en el sistema UPS, y fallas debidas a la emanación de hidrógeno	3	3	3	9
	B Fallos en el desempeño	3	B1 Falta de mantenimiento	3			

Tabla Nº 6.3: *Análisis y Evaluación del riesgo.*
Elaborado por: *Tania Guachi*

f) Tratamiento del riesgo.

El análisis y evaluación riesgo nos permitió valorizar el riesgo y conocer cuáles son los activos de información que están expuestos por lo tanto podemos saber a dónde enfocar los recurso del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., que se encuentran expuestos al riesgo.

El riesgo tiene 4 opciones de tratamiento que son:

- Reducir el riesgo, con la aplicación de contramedidas o salvaguardas especificadas controles del Anexo A de la norma.
- Evitar el riesgo, dejando de realizar la actividad que produce el riesgo.
- Transferir el riesgo, a un tercero como por ejemplo una aseguradora o una tercerización de servicios.
- Aceptar el riego, que consiste en asumir la responsabilidad de correr dicho riesgo.

La opción de aceptación de un riesgo deber ser aprobada formalmente por la dirección de la compañía, en la mayoría de casos se presenta esta situación cuando el control necesario de implantar tiene un valor económico que el mismo activo.

En nuestro caso la única opción de tratamiento que se usó fue la de reducción del riesgo.

g) Selección de controles.

Los controles son las contramedidas o salvaguardas especificadas en el Anexo A de la Norma ISO 27001:2005, enfocados a los 11 dominios de cobertura de la norma, como son:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Gestión de activos.

- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y ambiental.
- A.10 Gestión de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.13 Gestión de incidentes en seguridad de la información.
- A.14 Gestión de la continuidad del negocio.
- A.15 Cumplimiento.

La selección de los controles que la organización debe implementar se lo hace:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.

- Los requerimientos legales (implementación no es discutible).

Se ha tomado como referenciar a la ISO 17799:2005 actualmente conocida como ISO 27002 para una ampliación de las prácticas para implementar los controles e incluido los controles sugeridos por el Jefe del Departamento de Sistemas.

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Computadores de Oficina	A Virus	4	A1 Falta de mantenimiento	4	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.11.2 Gestión del acceso del usuario A.10.10 Monitoreo	A.9.2.4 Mantenimiento de Equipo (A1) A.11.2.3 Gestión de la clave del usuario (A2) A.10.10.2 Uso del sistema de monitoreo (B1,C1,D1)
			A2 Falta de controles de acceso	3						
	B Spyware	3	B1 Abuso del internet	2						
			B2 Falta de control de acceso	3						
	C Phishing	2	C1 Falta de herramientas de monitoreo	3						
	D Malware	3	D1 Abuso del Internet	3						
Switch	A Recalentamiento	3	A1 Falta de mantenimiento.	4	3	3	9	**Reducción del riesgo**	A.9.2 Seguridad del equipo	A.9.2.4 Mantenimiento de equipo (A1) A.9.2.1 Ubicación y protección del equipo (A2)
			A2 Flujo de energía.	4						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Impresoras	A Cartucho de impresión dañados	4	A1 Falta de mantenimiento	4	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo	A.9.2.4 Mantenimiento de equipo (A1, B1)
	B. Papel atascado	3	B1 Exceso de impresiones	3						
Router	A Virus	4	A1 Falta de mantenimiento	4	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.10.10 Monitoreo	A.9.2.4 Mantenimiento de equipo (A1) A.10.10.2 Uso del sistema de monitoreo(A2,B1)
			A2 Falta de instalación de programas de monitoreo	4						
	B Rendimiento	3	B1 Mucho tráfico del internet	4						
Servidor usado para servicios Web: Cajeros Móviles Web service de interfaz a buró de crédito	A Robo de información	4	A1 Falta de monitoreo	4	3	4	12	**Reducción del riesgo**	A.10.10 Monitoreo A.9.2 Seguridad del equipo	A.10.10.2 Uso del sistema de monitoreo(A1) A.10.10.3 Protección de la información del registro(A1) A.9.2.4 Mantenimiento de equipo (B1)
	B Desfiguración de la página web	4	B1 Falta de mantenimiento	3						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Bridge	A Ineficiencia	3	A1 Grandes interconexiones de redes	3	5	3	15	**Reducción del riesgo**	A.10.6 Gestión de seguridad de redes	A.10.6.1 Controles de red (A1) A.10.6.2 Seguridad de los servicios de red (A2)
			A2 saturación de las redes por tráfico de difusión	3						
Servidor que aloja el sistema y la base de datos del Software de Prevención de lavado de Activos	A Alteración y/o pérdida de los datos	4	A1 Escasas medidas de seguridad	4	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.10.10 Monitoreo	A.9.2.1 Ubicación y protección del equipo (A1,A2) A.10.10.2 Uso del sistema de monitoreo(A1) A.10.10.3 Protección de la información del registro(A1)
			A2 Imposición de restricciones	4						
Servidor de Base de Datos Sistema Sifiz y servidor de contingencias de sistema Sifiz	A Alteración y/o pérdida de los datos	4	A1 Escasas medidas de seguridad	4	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.10.10 Monitoreo	A.9.2.1 Ubicación y protección del equipo(A1,A2) A.10.10.2 Uso del sistema de monitoreo(A1) A.10.10.3 Protección de la información del registro(A1)
			A2 Imposición de restricciones	4						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Servidor de aplicaciones Sifiz institucional (Core financiero) y servidor de contingencias de BD institucional	A Alteración y/o pérdida de los datos	4	A1 Escaso medidas de seguridad	4	4	4	16	**Reducción del riesgo**	A.10.10 Monitoreo A.9.2 Seguridad del equipo A.8 Seguridad de RRHH	A.10.10.2 Uso del sistema de monitoreo(A1) A.10.10.3 Protección de la información (A1) A.9.2.4 Mantenimiento de Equipo(B1) A.8.1.1 Roles y Responsabilidades (B2)
	B Mal funcionamiento del sistema	4	B1 Falta de mantenimiento	3						
			B2 Mal uso por parte de los usuarios	4						
Servidor que aloja los blades de software Check Point Firewall IPS IDS VPN	A Ineficiencia	3	A1 Mala administración	3	5	3	15	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.11.5 Control de acceso al sistema de operación A.12.2 Procesamiento correcto en las aplicaciones A.10.10 Monitoreo	A.9.2.4 Mantenimiento de equipo (A1) A.11.5.4 Uso de utilidades del sistema (A1) A.12.2.2 Control de procesamiento interno (A1) A.10.10.2 Uso del sistema de monitoreo(B1) A.10.10.3 Protección de la información del registro(B1)
	B Alteración y/o pérdida de los datos	3	B1 Escaso de medidas de seguridad.	3						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Servidor de interface servicios de terceros con el Banco del Austro: Cajeros Automáticos Tarjetas de débito Chequeras	A Sin servicio	4	A1 Falla de conexión	4	4	4	16	**Reducción del riesgo**	A.6.2 Entidades externas	A.6.2.1 Identificación de riesgos relacionados con entidades externas (A1) A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes (A1).
Servidor que alojará el controlador de dominio institucional	A Error en autentificación de los usuarios	4	A1 Infracción en el manejo de controlador del dominio institucional	3	3	4	12	**Reducción del riesgo**	A.11.1 Requerimiento comercial para el control de acceso A.11.2 Gestión del acceso del usuario A.11.6 Control de acceso a la aplicación	A.11.1.1 Política de control de acceso (A1, A2) A.11.2.4 Revisión de los derechos de acceso del usuario (A1) A.11.6.1 Restricción al acceso a la información (A2)
			A2 Escaso de políticas de seguridad	4						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Servidor de contingencias de BD y aplicaciones ubicado en la oficina Salcedo	A Desactualización	4	A1 Falta de actualización de datos y de información	4	3	4	12	**Reducción del riesgo**	A.14 Gestión de la continuidad comercial	A.14.1.5 Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales (A1)
Software para cajero automático	A Inseguridad	4	A1 Falta de mecanismos de seguridad	4	3	4	12	**Reducción del riesgo**	A.12.5 Seguridad en los procesos de desarrollo y soporte A.12.4 Seguridad de los archivos del sistema A.9.2 Seguridad del equipo	A.12.5.4 Filtración de Información (A1, B1) A.12.4.1 Control de software operacional (B2) A.9.2.4 Mantenimiento de Equipo (B3)
	B Sin servicio	3	B1 Acceso no autorizado	3						
			B2 Manipulación errónea del sistema	3						
			B3 Falta de mantenimiento	4						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Software cuentas corrientes	A Datos erróneos	3	A1 Alteración de los datos	3	3	3	9	**Reducción del riesgo**	A.10.10 Monitoreo	A.10.10.3 Protección de la información del registro(A1) A.10.10.5 Registro de Fallas (A1)
Sistema financiero sifiz	A Intercepción e Interrupción	4	A1 Falta de planes de contingencia	3	3	4	12	**Reducción del riesgo**	A,6 .1 Organización interna A.5.1 Política de seguridad de información A.9.2 Seguridad del equipo A.10.10 Monitoreo	A.6.1.8 Revisión independiente de la seguridad de la información (A1) A.5.1.1 Documentar política de seguridad de información(A2) A.5.1.2 Revisión de la política de seguridad de la información (A2) A.9.2.4 Mantenimiento de Equipo(B1) A.10.10.2 Uso del sistema de monitoreo(B2)
			A2 Falta de políticas de accesibilidad	3						
	B Modificación	3	B1Falta de mantenimiento	3						
			B2 Falta de herramientas de seguridad	4						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Programa interface ahorros , tarjetas y cuentas corrientes	A Sin servicio	3	A1 Falta de mantenimiento	3	3	3	9	**Reducción del riesgo**	A.10.7 Gestión de medios	A.10.7.3 Procedimientos de manejo de la información (A1)
Software check point security bundle (firewall)	A Ineficiencia	4	A1 Mal Uso	3	3	4	12	**Reducción del riesgo**	A.10.7 Gestión de medios A.10.3 Planeación y aceptación del sistema	A.10.7.3 Procedimientos de manejo de la información (A1,,A2,A3) A.10.3.1 Gestión de Capacidad(B1)
			A2 Mala configuración	4						
			A3 Mala administración	4						
	B Fallas en el software	4	B1Falta de mantenimiento	3						
Equipos tape backup 100 gb para respaldar información	A Daños físicos	4	A1 Mal funcionamiento	3	3	4	12	**Reducción del riesgo**	A.9.2 Seguridad del equipo A.7 Gestión de activos A.11.3 Responsabilidades del usuario	A.9.2.1 Ubicación y protección del equipo (A1) A.7.1.3 Uso aceptable de los activos (A2,A3) A.11.3.2 Equipo de usuario Desatendido(B1)
			A2 Mal uso	3						
			A3 Método erróneo de almacenamiento del dispositivo	3						
	B Escases de Cintas	3	B1 Desatención	3						

Activo	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total riesgo	Opción de tratamiento de riesgo	Objetivos de control	Controles de la norma ISO 27001 (Control Vulnerabilidad)
Ups	A Contaminantes peligrosos suspendidos en el aire	3	A1 Situaciones de riesgo para el personal y/o falta de confiabilidad en el sistema UPS, y fallas debidas a la emanación de hidrógeno	3	3	3	9	**Reducción del riesgo**	A.9 Seguridad física y ambiental A.9.2 Seguridad del equipo	A.9.1.4 Protección contra amenazas externas y ambientales (A1) A.9.1.5 Trabajo en áreas Seguras (A1) A.9.2.4 Mantenimiento de Equipo(B1)
	B Fallos en el desempeño	3	B1 Falta de mantenimiento	3						

Tabla Nº 6.4: *Selección de controles.*
Elaborado por: *Tania Guachi*

h) Preparación de la declaración de aplicabilidad

Uno de los requerimientos de la norma ISO 27001:2005 es que la organización cuente con una DECLARACION DE LA APLICABILIDAD, que consiste en un documento que comprometa e identifique los controles del anexo A de la Norma que se implementarán y la justificación en caso de que no proceda. Esto significa que por defecto todos los controles de la norma son aplicables a la organización y cualquier excepción debe ser justificada. La declaración de aplicabilidad esta revisada y aprobada por el Jefe del Departamento de Sistemas.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	**No**	
A.5.1 Política de seguridad de información	A.5.1.1 Documentar política de seguridad de información	x		Es necesario definir políticas accesibilidad a nivel de información.
	A.5.1.2 Revisión de la política de seguridad de la información	x		
A.6.1 Entidades internas	A.6.1.8 Revisión independiente de la seguridad de la información	x		Es necesario manejar una adecuada organización en cuanto a la seguridad de la información
A.6.2 Entidades externas	A.6.2.1 Identificación de riesgos relacionados con entidades externas	x		Es recomendable aplicar medidas de seguridad en cuanto a los medios externos por los cuales se administra y se procesa información.
	A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes.	x		
A.7 Gestión de activos.- Responsabilidad por los activos.	A.7.1.3 Uso aceptable de los activos	x		Para mantener y mejorar la seguridad de los activos se debe identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.8 Seguridad de los recursos humanos	A.8.1.1 Roles y responsabilidades	x		Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados para tener control y seguridad en la información.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
A.9 Seguridad física y ambiental	A.9.1.4 Protección contra amenazas externas y ambientales	x		Es necesario llevar un control de seguridad en cuanto al acceso físico no autorizado, daño e interferencia al local y a la información.
	A.9.1.5 Trabajo en áreas Seguras	x		
A.9.2 Seguridad del equipo	A.9.2.1 Ubicación y protección del equipo	x		Es necesario mejorar la seguridad del equipo con el propósito de evitar la pérdida, daño, robo de los activos y la interrupción de las actividades de la organización
	A.9.2.4 Mantenimiento de Equipo	x		
A.10.3 Planeación y aceptación del sistema	A.10.3.1 Gestión de Capacidad	x		Es necesario realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.6 Gestión de seguridad de redes	A.10.6.1 Controles de red.	x		Es necesario implantar medidas de seguridad para asegurar la protección de la información en redes y de la infraestructura de soporte.
	A 10.6.2 Seguridad de los servicios de red.	x		
A.10.7 Gestión de medios	A.10.7.3 Procedimientos de manejo de la información.	x		Es recomendable definir procedimientos para el manejo y almacenaje de la información y así evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
A.10.10 Monitoreo	A.10.10.2 Uso del sistema de monitoreo.	x		Es recomendable establecer procedimientos para monitorear el uso de los medios de procesamiento de información.
	A.10.10.3 Protección de la información del registro.	x		
	A.10.10.5 Registro de Fallas	x		
A.11.1 Requerimiento comercial para el control del acceso	A.11.1.1 Política de control de acceso.	x		Es necesario establecer medidas de seguridad en cuanto al acceso a la información
A.11.2 Gestión del acceso del usuario	A.11.2.3 Gestión de la clave del usuario.	x		Es recomendable establecer medidas de seguridad para evitar el acceso no autorizado a los sistemas de información.
	A.11.2.4 Revisión de los derechos de acceso del usuario.	x		
A.11.3 Responsabilidades del usuario	A.11.3.2 Equipo de usuario desatendido	x		Es necesario solicitar a los usuarios que se aseguren de dar la protección apropiada al equipo desatendido
A.11.5 Control de acceso al sistema de operación	A.11.5.4 Uso de utilidades del sistema.	x		En necesario establecer seguridad en cuanto al uso restringido de los programas que podrían superar al sistema y los controles de aplicación.
A.11.6 Control de acceso a la aplicación e información	A.11.6.1 Restricción al acceso a la información.	x		Se debe aplicar seguridad en cuanto al acceso de los usuarios a los sistemas de información.

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
A.12.2 Procesamiento correcto en las aplicaciones	A.12.2.2 Control de procesamiento interno.	x		Es necesario establecer chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información en los sistemas de información.
A.12.4 Seguridad de los archivos del sistema	A.12.4.1 Control de software operacional.	x		Es necesario adoptar procedimientos para garantizar la seguridad de los archivos del sistema.
A.12.5 Seguridad en los procesos de desarrollo y soporte	A.12.5.4 Filtración de Información.	x		Es indispensable mantener la seguridad del software e información del mismo evitando oportunidades de filtraciones en la información.
A.14 Gestión de la continuidad comercial	A.14.1.5 Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales.	x		Es preciso realizar planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.

Tabla Nº 6.5: *Declaración de aplicabilidad*
Elaborado por: *Tania Guachi*

Revisado por: Ing. Diego Torres (Jefe del Departamento de Sistemas)

6.9.1.2 Implementar y operar el SGSI

a) Plan de tratamiento de riesgos.

Un plan de tratamiento de riesgos conlleva a la implantación en la organización de una serie de controles de seguridad con el objetivo de mitigar los riesgos no asumidos por la Dirección.

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados.

El Área de sistemas es responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de todo el departamento. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

c) Implementación de los controles seleccionados del ANEXO A

1. Política de Seguridad de la información

Seguridad lógica

Identificación

Evitar las violaciones de seguridad por ejemplo con claves compartidas para accesos críticos como la base de datos o servidores críticos accesibilidad física restringida al área de equipos.

El Operador de entorno de producción deberá realizar un chequeo mensual de los usuarios del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos. Las reglas de

contraseñas listadas a continuación están de acuerdo a los requerimientos y estándares internacionales.

La no definición de confidencialidad de la información puede provocar ciertos vacíos a la hora de asignar accesos.

Se debe definir contraseñas de acceso a nivel de información.

Contraseñas

La contraseña de verificación de identidad no debe ser trivial o predecible, y debe:

- Ser de al menos 8 caracteres de longitud.
- Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
- No contener un usuario ID como parte de la contraseña.
- Sistemas y aplicaciones que contengan información confidencial requiere que se cambie de contraseña al menos cada tres meses.

2. Organización de la seguridad de la información

Para fomentar la seguridad de la información se debe asegurar que los recursos el sistema de información (Software, hardware y datos) de una organización sean utilizados de la manera como se planeó.

Debe existir un compromiso de la gerencia con la seguridad de la información, coordinación de la seguridad de información, para los medios de procesamiento de información, acuerdos de confidencialidad, contacto con autoridades, contacto con grupos de interés y revisión independiente de la seguridad de la información

Organización interna.

Objetivo: Manejar la seguridad de la información internamente.

Se debe establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.

- **Revisión independiente de la seguridad de la información**

  Se debe revisar el enfoque del departamento para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.

  Esta revisión independiente es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque del departamento para manejar la seguridad de la información. La revisión debe incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.

  Si la revisión independiente identifica que el enfoque y la implementación del departamento de la organización para manejar la seguridad de la información no son adecuadas o no cumplen con la dirección para la seguridad de la información establecida en el documento de la política de seguridad de la información, la gerencia debe considerar acciones correctivas.

Entidades externas

Objetivo: Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.

La seguridad de la información y los medios de procesamiento de la información de la organización no deberán ser reducidos por la introducción de productos y servicios de grupos externos.

Se debe controlar cualquier acceso a los medios de procesamiento de información de la organización y el procesamiento y comunicación de la información realizado por grupos externos.

- **Identificación de los riesgos relacionados con los grupos externos**

  Se debe identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se deberá implementar controles apropiados antes de otorgarles acceso.

  Donde existe la necesidad de permitir que un grupo externo tenga acceso a los medios de procesamiento de la información o la información de una organización, se deberá llevar a cabo una evaluación del riesgo para identificar cualquier requerimiento de controles específicos

  No se debe otorgar acceso a los grupos externos a la información de la organización hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato definiendo los términos y condiciones para la conexión o acceso y el contrato de trabajo.

  Se debe asegurar que el grupo externo esté al tanto de sus obligaciones y acepte las responsabilidades involucradas en tener acceso, procesar, comunicar o manejar la información y los medios de procesamiento de información de la organización.

- **Tratamiento de la seguridad cuando se lidia con clientes**

  Se deberá tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

  Se debe considerar los siguientes términos de seguridad antes de proporcionar a los clientes acceso a cualquier activo de la organización (dependiendo del tipo y extensión de acceso dado, tal vez no se apliquen todos ellos):

  a) protección de activos, incluyendo:

     1. procedimientos para proteger los activos de la organización, incluyendo información y software, y el manejo de las vulnerabilidades conocidas;

     2. procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos, por ejemplo, una pérdida o modificación de datos;

     3. medidas de integridad;

     4. restricciones sobre el copiado y divulgación de información;

  b) la descripción del servicio o producto disponible;

  c) las diferentes razones, requerimientos y beneficios para el acceso del cliente;

  d) política de control de acceso;

  e) acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad;

f) una descripción de cada servicio que deberán estar disponible;

g) el derecho a monitorear, y revocar, cualquier actividad relacionada con los activos de la organización;

h) las respectivas obligaciones de la organización y el cliente;

i) responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de datos, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países;

j) derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor y protección de cualquier trabajo cooperativo.

Los requerimientos de seguridad relacionados con el acceso del cliente a los activos organizacionales pueden variar considerablemente dependiendo de los medios de procesamiento de la información y la información a la cual se tiene acceso. Estos requerimientos de seguridad pueden ser tratados utilizando acuerdos con el cliente, los cuales contienen todos los riesgos identificados y los requerimientos de seguridad. Los acuerdos con los grupos externos también pueden involucrar a otras partes interesadas. Los acuerdos que otorgan acceso a grupos externos debieran incluir el permiso para la designación de otras partes elegibles y condiciones para su acceso y participación.

3. Gestión de activos

- **Uso aceptable de los activos**

Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información. Todos los empleados, contratistas y

terceros deberán seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, incluyendo:

a) reglas para la utilización del correo electrónico e Internet;

b) lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local del departamento.

c) acceso a la red interna a través de VPNs (clientes móviles), o accesos remotos.

Los empleados, contratistas y terceros que usan o tienen acceso a los activos de la organización deberán estar al tanto de los límites existentes para su uso de la información y los activos asociados con los medios y recursos del procesamiento de la información de la organización. Ellos son los responsables por el uso que le den a cualquier recurso de procesamiento de información, y de cualquier uso realizado bajo su responsabilidad**.**

4. Seguridad de los recursos humanos

- **Roles y responsabilidades**

Se debe definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información. Tomar en cuenta el manual de funciones existente que detalla las funciones de cada cargo

Los roles y responsabilidades deben incluir requerimientos para:

a) implementar y actuar en concordancia con las políticas de seguridad de la información del departamento de la organización;

b) proteger los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada;

c) ejecutar procesos o actividades de seguridad particulares;

d) asegurar que se asigne a la persona la responsabilidad por las acciones tomadas; Explicación: Aquí la palabra "empleo" se utiliza para abarcar las siguientes situaciones diversas: Empleo de personas (temporal o permanente), asignación de roles de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

e) reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización. Los roles y responsabilidades de la seguridad deben ser definidos y claramente comunicados a los candidatos para el puesto durante el proceso de pre-empleo.

f) Se debe cuidar el tema de días y horarios de accesos

5. Seguridad física y ambiental

- **Protección contra amenazas externas e internas**

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre. Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle. También hay que considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no se deben almacenarse en el área asegurada;

b) el equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c) se debe proporcionar equipo contra-incendios ubicado adecuadamente.

- **Trabajo en áreas aseguradas**

Se debe diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas. Se debe considerar los siguientes lineamientos:

a) el personal debe estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer;

b) se debe evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos;

c) las áreas aseguradas vacías deben ser cerradas físicamente bajo llave y revisadas periódicamente;

d) no se debe permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado;

e) considerar el tema de que los equipos deben estar debidamente asegurados monetariamente con una empresa para el efecto.

Los arreglos para trabajar en las áreas aseguradas incluyen controles para los empleados, contratistas y terceros que trabajen en el área asegurada, así como otras actividades de terceros que allí se realicen.

6. Seguridad del equipo

- **Ubicación y protección del equipo**

Se debe ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado. Se debe considerar los siguientes lineamientos para la protección del equipo:

a) el equipo se debe ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;

b) los medios de procesamiento de la información que manejan datos confidenciales deben ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y se debe asegurar los medios de almacenaje para evitar el acceso no autorizado;

c) se debe aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;

d) se debe adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

e) se debe establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;

f) se debe monitorear las condiciones ambientales; tales como temperatura y humedad, que pueden afectar adversamente la operación de los medios de procesamiento de la información;

g) se debe aplicar protección contra rayos a todos los edificios y se debe adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;

h) se debe considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;

i) se debe proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

j) considerar el uso de software o hardware de respaldo de información crítica de por ejemplo, gerentes y jefes departamentales

- **Mantenimiento de equipo**

Se debe mantener correctamente el equipo para asegurar su continua disponibilidad e integridad. Se debe considerar los siguientes lineamientos para el mantenimiento de equipo:

a) el equipo se debe mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor;

b) sólo el personal de mantenimiento autorizado debe llevar a cabo las reparaciones y dar servicio al equipo;

c) se debe mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo;

d) se debe implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si

el mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario, se debe revisar la información confidencial del equipo, o se debe verificar al personal de mantenimiento.

e) considerar mantenimiento especializado para servidores y equipos críticos.

7. Planeación y aceptación del sistema

- **Gestión de Capacidad**

Los gerentes deben asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deben migrar a la producción después de obtener la aceptación formal. Se debe considerar los siguientes ítems antes de proporcionar la aceptación formal:

a) los requisitos de rendimiento y capacidad de los computadores;
b) los procedimientos de recuperación de errores y reinicio, así como los planes de contingencia;
c) la preparación y prueba de procedimientos operativos de rutina según las normas definidas;
d) un conjunto acordado de controles y medidas de seguridad instalados;
e) manual de procedimientos eficaz;
f) arreglos para la continuidad del negocio;
g) evidencia que la instalación del sistema nuevo no afectará adversamente los sistemas existentes, particularmente en las horas picos del procesamiento, como fin de mes;
h) evidencia que se está tomando en consideración el efecto que tiene el sistema nuevo en la seguridad general de la organización;

i) capacitación para la operación o uso de los sistemas nuevos;
j) facilidad de uso, ya que esto afecta el desempeño del usuario y evita el error humano.

Para los desarrolladores nuevos importantes, la función de las operaciones y los usuarios deben ser consultados en todas las etapas del proceso del desarrollo para asegurar la eficiencia operacional del diseño del sistema propuesto. Se debe llevar a cabo las pruebas apropiadas para confirmar que se ha cumplido totalmente con el criterio de aceptación.

8. Gestión de seguridad de redes

- **Controles de red**

Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.

Se debe implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadores, así como la protección de los servicios conectados contra accesos no autorizados. En particular, se debe considerar los controles y medidas siguientes:

a) La responsabilidad operativa de las redes deben estar separada de la operación de los computadores si es necesario;

b) Se debe establecer responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios;

c) Se debe establecer, si procede, controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados y también se deberían requerir controles y medidas especiales para mantener la

disponibilidad de los servicios de las redes y de los computadores conectados;

d) Un registro y monitoreo apropiado debe ser aplicado para permitir el registro de acciones relevantes de seguridad;

e) Se debe coordinar estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información.

- **Seguridad en los servicios de redes**

Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificadas e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización.

La habilidad del proveedor del servicio de red para manejar servicios acordados de una manera segura debe ser determinada y monitoreada regularmente, y el derecho para auditar debe ser acordado. Los acuerdos de seguridad necesarios para servicios particulares, como características de seguridad, niveles de servicio y los requisitos de gestión, deben ser identificados. La organización debe asegurarse que los proveedores del servicio de red implementen estas medidas.

9. Gestión de medios

- **Procedimientos de manejo de la información.**

Se debe establecer procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación. Los siguientes ítems deben ser considerados:

a) etiquetado en la administración de todos los medios;

b) restricciones de acceso para identificar al personal no autorizado;

c) mantenimiento de un registro formal de recipientes autorizados de datos;

d) aseguramiento de que los datos de entrada, su proceso y la validación de la salida están completos;

e) protección de los datos que están en cola para su salida en un nivel coherente con su criticidad;

f) almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante;

g) minimizar la distribución de datos;

h) identificación clara de todas las copias de datos para su atención por el receptor autorizado;

i) revisión de las listas de distribución y de receptores autorizados a intervalos regulares

10. Monitoreo

Se debe monitorear los sistemas y registrar los eventos de seguridad de la información. Los registros de operador y la actividad de registro de fallas se deben utilizar para garantizar la identificación de los problemas del sistema de información. Es recomendable emplear el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

- **Uso del sistema de monitoreo.**

Es necesaria la utilización de procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados.

Las áreas que se deben considerar incluyen:

a) acceso autorizado, incluyendo detalles tales como:

    1. ID del usuario;

    2. fecha y hora de los eventos claves;

    3. tipos de eventos;

    4. archivo a los cuales se tuvo acceso;

    5. programas/utilidades utilizados;

b) todas las operaciones privilegiadas, tales como:

    1. uso de las cuentas privilegiadas; por ejemplo, supervisor, raíz,, administrador;

    2. inicio y apagado del sistema;

    3. dispositivo I/O para adjuntar y eliminar lo adjuntado;

c) intentos de acceso no autorizado, como:

    1. accesiones del usuario fallidas o rechazadas;

    2. acciones fallidas o rechazadas que involucren los datos y otros recursos;

    3. violaciones a la política de acceso y notificaciones para los 'gateways' y 'firewalls' de la red;

    4. alertas de los sistemas de detección de intrusiones;

d) alertas o fallas del sistema como:

    1. alertas o mensajes en la consola;

    2. excepciones del registro del sistema;

3. alarmas de la gestión de la red;

4. alarmas activadas por el sistema de control de acceso;

5. cambios o intentos de cambio en los marcos y controles del sistema de seguridad.

La frecuencia con que se revisan los resultados de las actividades de monitoreo dependerá de los riesgos involucrados. Los factores de riesgo a considerarse incluyen:

a) grado crítico de los procesos de aplicación;

b) valor, sensibilidad y grado crítico de la información involucrada;

c) antecedentes de infiltración y mal uso del sistema, y la frecuencia con la que se explotan las vulnerabilidades;

d) extensión de la interconexión del sistema (particularmente las redes públicas);

e) desactivación del medio de registro.

- **Protección del registro de información**

Los controles deben tener el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro debe incluir:

a) las alteraciones registradas a los tipos de mensajes;

b) los archivos de registro que se editan o borran;

c) capacidad de almacenamiento del medio de archivos de registro que se está excediendo, resultando en una falla en el registro de eventos o la escritura encima de los eventos registrados en el pasado.

- **Registro de fallas**

Los registros deben incluir;

a) la hora la cual ocurre un evento (éxito o falla);

b) la información sobre el evento (por ejemplo, archivos manejados) o falla (por ejemplo, el erro ocurrido y la acción correctiva);

c) cuál cuenta y cuál operador o administrador está involucrado;

d) cuáles procesos están involucrados.

Los registros de administrador y operador del sistema deben ser revisados de manera regular.

11. Requerimiento comercial para el control del acceso

- **Política de control del acceso**

Las reglas de control del acceso y los derechos para cada usuario o grupos de usuarios se deben establecer claramente en la política de control de acceso. Los controles de acceso son tanto lógicos como físicos y estos deben ser considerados juntos.

La política debe tomar en cuenta lo siguiente:

a) los requerimientos de seguridad de las aplicaciones comerciales individuales;

b) identificación de toda la información relacionada con las aplicaciones comerciales y los riesgos que enfrenta la información;

c) consistencia entre el control del acceso y las políticas de clasificación de la información de los diferentes sistemas y redes;

d) los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización;

e) gestión de los derechos de acceso en un ambiente distribuido y en red que reconoce todos los tipos de conexiones disponibles;

f) segregación de roles del control del acceso; por ejemplo, solicitud de acceso, autorización de acceso, administración del acceso;

g) requerimientos para la autorización formal de las solicitudes de acceso;

h) requerimientos para la revisión periódica de los controles de acceso

i) revocación de los derechos de acceso.

12. Gestión del acceso del usuario

- **Gestión de la clave del usuario.**

El proceso de gestión del acceso del usuario se debe incluir los siguientes requerimientos:

a) se debe requerir que los usuarios firmen un enunciado para mantener confidenciales las claves secretas y mantener las claves secretas grupales sólo dentro de los miembros el grupo; este enunciado firmado se puede incluir en los términos y condiciones de empleo;

b) cuando se requiere que los usuarios mantengan sus propias claves secretas, inicialmente se les debe proporcionar una clave secreta temporal segura, la cual están obligados a cambiar inmediatamente;

c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nuevo, sustituta o temporal;

d) las claves secretas temporales deben ser proporcionadas a los usuarios de una manera segura, se debe evitar el uso de mensajes de correo electrónico de terceros o no protegidos;

e) las claves secretas temporales deben ser únicas para la persona y no deben ser fáciles de adivinar;

f) los usuarios deben reconocer la recepción de las claves secretas;

g) las claves secretas nunca deben ser almacenadas en los sistemas de cómputo de una forma desprotegida;

h) las claves secretas predeterminadas por el vendedor deben ser cambiadas después de la instalación de sistemas o software

- **Revisión de los derechos de acceso del usuario**

La revisión de los derechos de acceso debe considerar los siguientes lineamientos:

a) los derechos de acceso de los usuarios deben ser revisados por unidad de talento humano ó una unidad de riesgos ó por los jefes departamentales requirentes o dueños del proceso a intervalos regulares; por ejemplo, un período de 6 meses, y después de cualquier cambio, como un ascenso, democión o terminación del empleo;

b) los derechos de acceso del usuario se debe revisar y re-asignar cuando se traslada de un empleo a otro dentro de la misma organización;

c) las autorizaciones para derechos de acceso privilegiados especiales se debe revisar a intervalos más frecuentes; por ejemplo, un período de 3 meses;

d) se debiera chequear la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados;

e) se deben registrar los cambios en las cuentas privilegiadas para una revisión periódica.

13. Responsabilidades del usuario

- **Equipo de usuario desatendido**

Los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada.

Todos los usuarios deben estar al tanto de los requerimientos de seguridad y los procedimientos para proteger el equipo desatendido, así como las responsabilidades para implementar dicha protección. Se debe comunicar a los usuarios lo siguiente:

a) cerrar las sesiones activas cuando se termina, a no ser que puedan asegurarse con un mecanismo de cierre apropiado; por ejemplo, protector de pantalla asegurado mediante clave secreta;

b) salir de las computadoras mainframe, servidores y PCs de oficina cuando se termina la sesión (es decir, no sólo apagar la pantalla de la PC o Terminal);

c) asegurar las PCs o terminales contra un uso no autorizado mediante un seguro con clave o un control equivalente; por ejemplo, acceso con clave secreta, cuando no está en uso.

14. Control de acceso al sistema de operación

Se debe considerar los siguientes lineamientos para el uso de las utilidades del sistema:

a) uso de los procedimientos de identificación, autenticación y autorización para las utilidades del sistema;

b) segregación de las utilidades del sistema del software de la aplicación;

c) limitar el uso de las utilidades del sistema a un número práctico mínimo de usuarios autorizados y confiables;

d) autorizar el uso de las facilidades con un propósito concreto (ad hoc);

e) limitar la disponibilidad de las utilidades del sistema; por ejemplo, por la duración de un cambio autorizado;

f) registro (logging) de todo uso de las utilidades del sistema;

g) definir y documentar los niveles de autorización de las utilidades del sistema;

h) eliminación o inutilizar todas las utilidades innecesarias basadas en software, así como los software del sistema que sean innecesarios;

i) no poner en disponibilidad las facilidades del sistema a usuarios que tenga acceso a aplicaciones en sistemas donde la segregación de tareas sea requerida.

j) definir funcionarios de Backup en el mismo manual de funciones.

15. Control de acceso a la aplicación e información

Las restricciones de acceso deben estar basadas en requisitos específicos de la aplicación y consistente con la política de acceso a la información de la organización.

Se debe considerar lo siguiente para dar soporte a los requisitos de restricciones de acceso:

a) establecer menús para controlar los accesos a las funciones del sistema de aplicaciones;

b) controlar los derechos de acceso de los usuarios, por ejemplo lectura, escritura, borrado, ejecución:

c) controlar los derechos de acceso de otras aplicaciones;

d) asegurarse que las salidas de los sistemas de aplicación que procesan información sensible, solo contienen la información correspondiente para el uso de la salida y se envían, únicamente, a los terminales y sitios autorizados, incluyendo la revisión periódica de dichas salidas para garantizar la supresión de información redundante.

16. Procesamiento correcto en las aplicaciones

- **Control de procesamiento interno.**

El diseño de las aplicaciones debe asegurar la implantación de restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad. Aéreas de riesgo específicas a considerar serian:

a) el uso en los programas de funciones "añadir" y "borrar" para cambiar los datos;

b) los procedimientos para evitar programas que corran orden equivocado o después del fallo de un proceso anterior;

c) el uso de los programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos;

d) la protección contra ataques utilizando corridas o desbordes de buffers.

Se debe tener preparado una lista de verificación apropiada, tener las actividades documentadas y los resultados deben mantenerse seguros. A continuación se dan ejemplos de comprobaciones que pueden incorporarse:

a) controles de sesión o de lotes, para conciliar los cuadres de los archivos tras la actualizaciones de las transacciones;

b) controles para comprobar los cuadros de apertura contra los cuadros previos del cierre, como:

- controles de corrida-a-corrida
- totales de actualización de archivos;
- controles de programa a programa;

c) validación de los datos generados por el sistema;

d) comprobaciones de la integridad, autenticidad u otro aspecto de seguridad de datos o del software transferidos entre el computador central y las computadoras remotas;

e) totales de comprobación de registro y archivos;

f) comprobaciones que aseguren que los programas se ejecutan en el orden correcto, que finalizan en caso de falla y que no sigue el proceso hasta que el problema se resuelve;

g) crear un registro de las actividades envueltas en el procesamiento.

17. Seguridad de los archivos del sistema

- **Control de software operacional.**

Para minimizar el riesgo de corrupción se debe considerar lo siguiente:

a) la actualización del software operacional, aplicaciones y bibliotecas de programas sólo debe ser realizada por administradores capacitados con la apropiada autorización gerencial;

b) los sistemas operacionales sólo deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

c) no se debe implantar código ejecutable en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuente. Deben ser realizadas en un sistema separado.

d) Se debe utilizar un sistema de control de configuración para mantener un control de todo el software implementado así como la documentación del sistema;

e) se debe mantener un registro de auditoría de todas las actualizaciones a las librerías de programas en producción;

f) se debe retener como un número de 5 de las versiones anteriores de software como medida de precaución para contingencias;

g) las versiones antiguas de software deben ser archivadas junto con toda la información requerida, los procedimientos, detalles de configuración y software de soporte durante el tiempo en que los datos sean retenidos.

18. Seguridad en los procesos de desarrollo y soporte

- **Filtración de Información.**

Se debe considerar los siguientes puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos:

a) escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida;

b) enmascarar y modular la conducta del sistema y las comunicaciones para reducir la probabilidad de que una tercera persona pueda deducir la información a partir de dicha conducta;

c) hacer uso de los sistemas y el software considerados de la más alta integridad; por ejemplo productos evaluados(ISO/IEC 15408);

d) monitoreo regular de las actividades del personal y del sistema, donde sea permitido bajo la legislación o regulación;

e) monitoreo del uso de recursos en sistemas de cómputo.

19. Gestión de la continuidad comercial

- **Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales.**

Las pruebas de los planes de continuidad del negocio deben asegurar que todos los miembros del equipo de recuperación y otro personal relevante están prevenidos de los planes y de sus responsabilidades para la continuidad del negocio y la seguridad de información. Todos deben saber su rol cuando el plan sea invocado.

Se debe elaborar un calendario de pruebas para plan(es) de continuidad del negocio, en el cual se debe indicar cómo, cuándo probar cada elemento del plan. Se recomienda probar los componentes individuales del plan con frecuencia.

Se debe utilizar diversas técnicas para proporcionar la seguridad de que los planes funcionarán en la vida real. Estas deberían incluir:

a) la prueba sobre el papel de varios escenarios (analizando las disposiciones de recuperación del negocio con ayuda de ejemplos de interrupciones);

b) las simulaciones (en particular para entrenar en sus respectivos para peles al personal que gestione la crisis tras la contingencia);

c) las pruebas de recuperación técnica (asegurando que los sistemas de información pueden restaurarse con efectividad);

d) las pruebas de recuperación en un lugar alternativo (haciendo funcionar los procesos del negocio en paralelo con las operaciones de recuperación fuera del lugar principal,

e) las pruebas de los recursos y servicios del proveedor (asegurando que los servicios externos proporcionados cumplen el compromiso contraído);

f) los ensayos completos (probando que pueden hacer frente a las interrupciones de la organización, el personal, los recursos y los procesos);

g) documento de pruebas realizadas con conclusiones y recomendaciones.

Se debe asignar responsabilidades para revisar regularmente cada plan de continuidad del negocio. Se debe hacer una actualización apropiada

del plan tras la identificación de cambios en las características del negocio no reflejadas en los planes de continuidad del negocio. Este proceso formal de control de cambios debe asegurar que las revisiones regulares del plan completo ayuden a reforzar y distribuir los planes actualizados.

Ejemplos de situaciones que necesitarían la actualización de planes: la adquisición de nuevos equipos o la mejora de los sistemas operativos con cambios en:

a) el personal;

b) las direcciones o números de teléfono;

c) las estrategias del negocio;

d) los lugares, dispositivos y recursos;

e) la legislación;

f) los contratistas, proveedores y clientes principales;

g) los procesos existentes, nuevos y clientes principales;

h) los riesgos (operativos o financieros).

a) Efectividad de los controles

Ref.	Objetivo	Actividades	Posibles Métricas
5. Política de seguridad			
5.1	**Política de seguridad de la información**	Revisiones semestrales del contenido y cumplimiento de las políticas establecidas para la seguridad de la información.	Definición y aceptación de políticas para la seguridad de la información. Aceptable un 80% mínimo
6. Aspectos organizativos de la seguridad de la información			
6.1	**Organización Interna**	• Revisión del enfoque del departamento para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) de manera independiente cada tres meses, o cuando ocurran cambios significativos en la implementación de la seguridad. • Asignación de roles y responsabilidades de seguridad de la información a los trabajadores del departamento	Porcentaje de funciones cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información. Porcentaje de empleados que han: Aceptado formalmente, roles y responsabilidades de seguridad de la información. Aceptable un 75% mínimo inicialmente
6.2	**Entidades Externas**	• Controlar y monitorear a las entidades externas. • Organizar y Mantener actualizada la cadena de los proveedores.	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras. Aceptable un 90% mínimo inicialmente

Ref.	Objetivo	Actividades	Posibles Métricas
7. Gestión de activos			
7.1	**Responsabilidad sobre** **los activos**	• Elaboración de inventarios de los activos de información en cada fase del proceso de clasificación (identificado/riesgo evaluado/ clasificado/ asegurado) • Revisar que los trabajadores del departamento realicen un uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, tales: a. reglas para la utilización del correo electrónico e Internet; b. lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local del departamento. c. acceso a la red interna a través de VPNs (clientes móviles), o accesos remotos.	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables. Aceptable un 75% mínimo inicialmente
8. Seguridad ligada a los recursos humanos			
8.1	**Antes de la contratación** **Roles y Responsabilidades**	Revisión del manual de funciones existente que detalla las funciones de cada cargo y verificar si se da cumplimiento lo que está definido y agregar las funciones que sean necesarias.	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar. Aceptable un 85% mínimo inicialmente
9. Seguridad física y ambiental			
9.1	**Áreas seguras**	• Dos revisiones anuales para verificar la seguridad física de instalaciones, incluyendo actualizaciones regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes. • Revisar los archivos logs de los medios biométricos.	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes. Aceptable un 85% mínimo inicialmente

Ref.	Objetivo	Actividades	Posibles Métricas
9.2	**Seguridad de los equipos**	• Elaborar una revisión mensual por muestreo, para verificar el estado y funcionamiento de los equipos. • Chequear el manual de políticas y procedimientos de seguridades físicas y lógicas. • Aplicar mantenimiento a los equipos de forma trimestral. • Verificar los planes de contingencia	Porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad. Máximo un 2% de chequeos con movimientos no autorizados
10. Gestión de comunicaciones y operaciones			
10.3	**Planificación y aceptación del sistema**	• Revisión los requisitos de rendimiento y capacidad de los computadores. • Mantener actualizados los manuales de procedimientos de los sistemas. • Definición de controles para verificar el análisis de riesgos realizados y evaluar los activos y considerar cambios o mejoras para mantener la seguridad de la información. • Desarrollar detallados criterios de aceptación de nuevos sistemas, actualizaciones y versiones que deban ser implantados.	Porcentaje de cambios de riesgo bajo, medio, alto y de emergencia. Máximo un 5% de cambios considerados de alto riesgo Número y tendencia de cambios revertidos y rechazados frente a cambios exitosos. Máximo un 5% de cambios rechazados Porcentaje de sistemas: (a) que deberían cumplir con estándares de seguridad básica o similares y Mínimo 90% de sistemas han adoptado controles de seguridad. (b) cuya conformidad con dichos estándares ha sido comprobada mediante benchmarking o pruebas. Mínimo un 75% se obtuvo de conformidad con los controles establecidos.

Ref.	Objetivo	Actividades	Posibles Métricas
10.6	**Gestión de la seguridad de las redes**	Monitorear y determinar los incidentes de seguridad de red identificados en el mes anterior. Asignar controles para evitar los incidentes de seguridad (correo electrónico y los archivos y carpetas a través de Encriptación) Monitorear, encontrar, registrar, y haga cumplir las políticas de la organización.	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa. Máximo 10 incidentes leves 5 importantes 0 graves
10.7	**Gestión de medios**	Elaborar soportes encriptados de backup de la información. Revisión de los privilegios de los usuarios de los sistemas de información. Concientizar a los empleados del departamento sobre la seguridad de la información	Porcentaje de soportes de backup o archivo que están totalmente encriptados. 50% de archivos encriptados inicialmente
10.10	**Monitoreo**	Monitorear las operaciones privilegiadas (cuentas privilegiadas, inicio y apagado del sistema) Registro de intentos no autorizados. Realizar revisiones periódicas y procedimientos de monitorización del uso de los sistemas.	Porcentaje de sistemas cuyos logs de seguridad: (a) están adecuadamente configurados, (mínimo 60% inicialmente) (b) son monitorizados/revisados/evaluados regularmente. (mínimo 55% inicialmente)

Ref.	Objetivo	Actividades	Posibles Métricas
11. Control de accesos			
11.1	**Requerimiento comercial para el control del acceso**	• Revisar el manual de políticas y procedimientos. • Monitorear el uso y funcionamiento de los activos de información.	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a)sido identificados, (mínimo 80% inicialmente) (b)aceptado formalmente sus responsabilidades, (mínimo 70% inicialmente) (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (mínimo 80% inicialmente) (d) definido las reglas de control de acceso basadas en roles. (mínimo 85% inicialmente)
11.2	**Gestión de acceso de usuario**	Chequear el manual de procedimientos y políticas propiamente definidos, para verificar si se están cumpliendo a cabalidad. Revisiones trimestrales sobre los accesos privilegiados de los usuarios. Revisar y mantener el ciclo de vida de acceso de los usuarios: • Registro de usuarios • Administración de privilegios • Administración de las contraseñas • Revisión de los derechos.	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos 48 horas Número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico / valle (ejemplo, "Implantada nueva aplicación financiera este mes"). 30 solicitudes de cambio promedio al mes

Ref.	Objetivo	Actividades	Posibles Métricas
11.3	**Responsabilidades del usuario**	• Revisar el plan de concientización de la información. • Comunicar a los usuarios de los activos sobre las responsabilidades que se les debe dar a los equipos desatendidos.	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información (a) totalmente documentada y (b) formalmente aceptada. (mínimo 80% de las descripciones de puesto deben involucrar responsabilidades de seguridad)
11.5	**Control de acceso al sistema de operación**	Verificación de la identificación, autenticación de los usuarios para los sistemas de información y de comunicación. • Revisar los archivos logs de los sistemas. • Definir funcionarios de Backup en el manual de funciones • Uso de utilitarios del sistema. • Limitación del horario de conexión • Revisar el manual de procedimientos y políticas de seguridad física y lógica.	Estadísticas de vulnerabilidad de sistemas y redes. (mínimo 90% de vulnerabilidades deben ser solventadas en un plazo no menor a 48 horas)
11.6	**Control de acceso a la aplicación e información**	• Revisar el manual de procedimientos y políticas de seguridades físicas y lógicas. • Revisar los archivos logs del sistema biométrico • Definición de controles de seguridad informática	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (ejemplo "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)". (mínimo 70% inicialmente)

Ref.	Objetivo	Actividades	Posibles Métricas
12. Adquisición, desarrollo y mantenimiento de los sistemas de información			
12.2	**Procesamiento correcto en las aplicaciones**	• Constatar el trabajo realizado por parte de los desarrolladores del departamento. • Asignar revisiones mensuales por parte del operador del Entorno. • Monitoreo	Porcentaje de sistemas para los cuales los controles de validación de datos se han (a) definido (mínimo 80% inicialmente) (b) implementado y demostrado eficaces mediante pruebas. (mínimo 70% inicialmente)
12.4	**Seguridad de los archivos del sistema**	• Revisar el manual de procedimientos de políticas. • Revisar, mantener y mejorar el análisis de riesgos de los activos. • Analizar ¿Cuáles son los directorios o archivos que no deben cambiar y cuáles sí? Pruebas de backtesting del funcionamiento del aplicativo.	Porcentaje de sistemas evaluados de forma independiente en cuanto a la seguridad de la información (confidencialidad, integridad, etc.) (mínimo 60% inicialmente)
12.5	**Seguridad en los procesos de desarrollo y soporte**	• Desarrollar un procedimiento de control de cambios. • Realización de revisiones técnicas a las aplicaciones luego de realizar cualquier cambio, teniendo especial atención a las aplicaciones críticas. • Documentar claramente las restricciones que se deben considerar en los cambios de paquetes de software. • Implementación de medidas tendientes a evitar fugas de información. Supervisión y monitorización de desarrollos de software externalizado. Administración técnica de vulnerabilidades	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc. (Se hallan definidas las políticas de evaluación de los sistemas de desarrollo se deberá evaluar el 95 % de los sistemas en desarrollo arrojando incidentes leves en máximo el 5%)

Ref.	Objetivo	Actividades	Posibles Métricas
14	**Gestión de la continuidad comercial**	• Revisar los planes de contingencia destinados para la continuidad del negocio. • Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales.	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). (mínimo 70% de las fases del ciclo de vida deben contener planes o procedimientos de contingencia) Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (mínimo 70% inicialmente) (b) probados mediante test apropiados en los últimos 12 meses. (mínimo 70% inicialmente)

Tabla Nº6.6: *Métricas de la ISO 27001*
Elaborado por*: Tania Guachi*

Revidado por: Ing. Diego Torres (Jefe del Departamento de Sistemas)

b) Implementar los programas de capacitación y conocimiento

El departamento debe asegurar que todo el personal del departamento sea competente para realizar las tareas requeridas para:

- Determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
- proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades;
- evaluar la efectividad de las acciones tomadas;
- mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros. Se deben mantener registros del desempeño del proceso y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.).

El departamento también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

f) Manejar recursos para el SGSI

Los recursos que compone el SGSI son los trabajadores del Departamento de sistemas de la Cooperativa (Jefe de Sistemas, Programadores, Administrador de Sistemas, y el Ayudante del Administrador de Sistemas) quienes son los

responsables de velar por la seguridad de los sistemas de información y de comunicación que existen en el departamento, así como también mantener activamente los servicios que ofrecen.

g) Implementar los procedimientos capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

Existen muchos modos de responder inmediatamente a un incidente de seguridad. Los siguientes pasos han sido formulados en función a cuándo y cómo reaccionar desde el momento en el que se anuncia un incidente de seguridad, mientras está ocurriendo y una vez ha concluido.

Paso 1: Informar sobre el incidente.

¿Qué ocurre/ha ocurrido? (intentar centrarse en los hechos compilados). ¿Dónde y cuándo ocurrió? ¿Quién está implicado? (en caso de que se pueda determinarlo) ¿La persona o propiedad ha sufrido algún tipo de daño o perjuicio?

Paso 2. Decidir cuándo reaccionar. Hay tres posibilidades:

Una reacción inmediata es necesaria cuando hay que atender a personas heridas o frenar un ataque en marcha. Una reacción rápida (en las próximas horas o incluso días) es necesaria cuando hay que prevenir que surjan nuevos posibles incidentes (el incidente en sí ya pasó). Una acción de seguimiento (en varios días o semanas o incluso meses): Si la situación se ha estabilizado, tal vez no resulte necesaria una reacción ni inmediata ni rápida, sino de seguimiento. Por lo mismo, también cualquier incidente de seguridad que haya requerido una reacción inmediata o rápida deberá someterse a observación a través de una acción de seguimiento para poder conservar nuestro espacio de trabajo o revisar nuestro contexto de actuación.

Paso 3. Decidir cómo reaccionar y cuáles son tus objetivos.

Si la reacción debe ser inmediata, los objetivos son claros: Atender a los heridos o frenar el ataque. Si la reacción debe ser rápida, los objetivos deberán ser establecidos por la persona encargada o el equipo de crisis (o similar) y deberá centrarse en restaurar la seguridad necesaria para los afectados por el incidente.

Las acciones/reacciones posteriores se llevarán a cabo siguiendo los canales habituales de la organización en la toma de decisiones, con el objetivo de restaurar un entorno de trabajo seguro, así como de re-establecer los procedimientos organizativos internos y mejorar las reacciones posteriores ante los incidentes de seguridad.

Toda reacción debe también tener presente la seguridad y protección de otras personas, organizaciones o instituciones con las que mantengamos una relación laboradle trabajo (y se puedan ver afectados).

Establecer objetivos antes de empezar a actuar. La inmediatez de la acción es importante, pero saber por qué llevar a cabo esa acción es más importante todavía. Al establecer de antemano qué pretendes lograr (objetivos), podrás decidir cómo quieres lograrlo (táctica a seguir).

6.9.1.3 Monitorear y revisar el SGSI

Se realizarán de forma trimestral y cuando se realicen modificaciones importantes a los procesos de negocios.

Actividades principales para esta fase, ellas son:

- Monitoreo
- Métricas
- Auditorías
- Revisión.

a) Monitoreo

A los efectos de detectar, posibles diferencias entre el estado de seguridad de la Organización (sujeto al Alcance definido para el SGSI) y el estado que se pretende alcanzar (objetivos y requerimientos de seguridad), es necesario recabar y recolectar datos precisos que permitan de forma objetiva posicionar el estado de seguridad en el departamento de sistemas.

Entrada:

- Alcance y Política del SGSI.
- Estándares y procedimientos relacionados a la Seguridad de la información.
- Resultado de la Evaluación de Riesgos
- Objetivos de Control.
- Controles seleccionados.
- Requerimientos específicos de la Seguridad de la Información.
- Clasificación de Procesos y Activos
- Registros de Incidentes de Seguridad de la Información.
- Estado de las Actividades planificadas y que se están llevando a cabo.

Acción:

Deben realizarse revisiones y chequeos en forma regular trimestral de verificar que se están aplicando adecuadamente todos los controles seleccionados. Deben coordinarse las acciones de monitoreo de forma de lograr su cometido minimizando su impacto en las operaciones de la empresa y sin que tenga un impacto en la calidad del servicio ni en los procesos diarios.

Las acciones de monitoreo deben ser tendientes a:

- Detectar problemas o desviaciones de los niveles deseados.
- Tomar acciones correctivas
- Eventualmente replantearse los procedimientos y soluciones técnicas.

Quienes deberían participar:

Trabajadores del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

Salida:

- Registro de todas las actividades de monitoreo y un informe en el cual sintetice el resultado de estas actividades.
- Un informe con las recomendaciones técnicas en función de los resultados obtenidos.

b) Métricas

De las métricas establecidas en el capítulo anterior revisarlas y analizarlas para ver si cumplen con sus parámetros establecidos.

c) Auditorías Internas del SGSI

Según la ISO/IEC 27.001, deben realizarse auditorías internas a intervalos planificados para determinar si los objetivos de control, controles, procesos y procedimientos cumplen:

- Los controles están implementados y se mantienen de forma eficaz
- Se desempeñan de acuerdo a lo esperado (eficiencia).

Debe documentarse, los criterios, el alcance, la frecuencia y los métodos que se llevarán a cabo.

Quienes deberían participar:

El grupo de trabajadores del Departamento de Sistemas de la Cooperativa:

- Planificar la auditoría que se llevará a cabo.
- Documentar los resultados.
- Proponer acciones correctivas y preventivas.

d) Revisión

Esta etapa o proceso, debe realizarse de forma trimestral y planificada, y tiene como objetivos:

- Evaluar la efectividad del SGSI
- Analizar los riesgos residuales
- Actualizar los planes de seguridad

Entrada:

- Resultados de las etapas de monitoreo en función de las métricas.
- Cambios en la realidad del negocio que afecten el SGSI
- Informes de auditoría interna.
- Posibles nuevas tecnologías aplicables a los controles existentes u otros nuevos.
- Sugerencias e informes recogidos acerca del SGSI.

Acción:

Realizar:

Revisar la vigencia de las premisas, principios y condiciones bajo cuales se tomaron las decisiones y criterios de definiciones del SGSI.

- ¿Es el alcance del SGSI adecuado y suficiente o conviene redefinirlo de acuerdo a la nueva realidad o nuevos objetivos?
- ¿Los niveles de seguridad definidos en cuanto a confidencialidad, disponibilidad e integridad son suficientes?
- ¿Los controles definidos e implementados son efectivos?
- ¿Las políticas de seguridad de la información están actualizadas?

- ¿Están los requerimientos de seguridad de la información alineados con los contratos con proveedores y clientes?
- ¿Ha cambiado el alcance y/o política del SGSI de la empresa principal?

Quienes deberían participar:

Grupo de trabajadores del departamento de sistemas de la cooperativa.

Salida:

- Informe de mejoras para hacer al SGSI más efectivo.
- Redefinir o ajustar el SGSI para adaptarse a los cambios de la realidad o simplemente para lograr los objetivos de control trazados.

6.9.1.4 Mantener y mejorar el SGSI

Es así que en esta etapa se debe tener en cuenta:

- Identificar no conformidades (del SGSI).
- Definir acciones correctivas y preventivas.
- Evaluar sugerencias y definir la implementación de mejoras.
- Comunicar estos cambios y mejoras.
- Monitorear la implementación de estos cambios.

Entrada:

- Informes de Auditoría interna.
- Informes de no conformidades que estén dentro del alcance del SGSI en cuestión.
- Informes de conclusiones y sugerencias surgidas de la etapa de revisión.
- Propuestas de mejoras de otras áreas y unidades de negocios.

Quienes deberían participar:

Grupo de trabajadores del departamento de sistemas

Acción:

- Se debe realizar las siguientes actividades:
- Identificación de no conformidades.
- Identificación de acciones correctivas y preventivas.
- Implementación de las mejoras.
- Testeo del logro de las mejoras esperadas.
- Monitoreo.
- Comunicación de los cambios y las mejoras.

Salida:

Un Informe con el plan de mejoras, describiendo o referenciando las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados así como un plan tentativo para llevarlos a cabo.

6.10 CONCLUSIONES Y RECOMENDACIONES

6.10.1 Conclusiones

- El contenido de la ISO 27001 está orientado al tratamiento de seguridad de la información mediante la gestión de riesgos, ya que describe la manera de mantener y mejorar la seguridad de los activos de información de cualquier organización.
- Para garantizar y mejorar la seguridad en cuanto a la confiabilidad, disponibilidad e integridad de la información en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda., se ha diseñado un Sistema de Gestión de Seguridad de la Información, en donde se ha determinado que algunos activos se encuentran desprotegidos por ende se ha definido controles que aseguren la protección de la información.
- Al tener implantado un SGSI bajo la norma ISO 27001 no significa contar con seguridad máxima en la información de la organización sino que esto significa que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

6.10.2 Recomendaciones

- Se recomienda extender el modelo de políticas de seguridad informática desde el departamento de sistemas a toda la cooperativa por supuesto se debe contar con el apoyo de la gerencia y debe ser un objetivo planteado para la cooperativa.
- Se recomienda revisar continuamente o por lo menos cada seis meses el sistema de gestión de seguridad de la información ya que esta en mejora continua.
- Debido a que la información es muy importante se recomienda que las empresas capaciten al personal referente a la norma de seguridad informática, y no verlo como un gasto sino como una inversión, ya que son muchos los beneficios obtenidos gracias a la aplicación de esta norma.

BIBLIOGRAFIA

Información bibliográfica de libros

- SENN, James A. (1997). Análisis y diseño de sistemas de Información. Divinni Editorial LTDA. Colombia.
- ZACKER, Craig (2002). Manual de referencia de redes. McGraw-Hill/Interamericana. España.
- STALLINGS, William. (2006). Sistemas Operativos. Pearson Educación S.A. Madrid.

Información bibliográfica de páginas web

- IMPLEMENTACIÓN DEL PRIMER SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, EN EL ECUADOR, CERTIFICADO BAJO LA NORMA (2009). Extraído el 18 de Julio de 2011 desde http://www.dspace.espol.edu.ec/bitstream/123456789/7718/1/D-39433.pdf
- ÁLVAREZ, María y GARCÍA, Pamela. IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA LA INTRANET DE LA CORPORACIÓN METROPOLITANA DE SALUD (2008). Extraído el 18 de Julio de 2011 desde http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1077.pdf
- LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS
- Y MENSAJES DE DATOS (2004). Extraído el 18 de Julio de 2011 desde http://sinar.gov.ec/downloads/L_comercio.pdf
- LEY DE PROPIEDAD INTELECTUAL (1988). Extraído el 18 de Julio de 2011 desde http://www.cetid.abogados.ec/archivos/archivos/index.php?p=boletin_mostrar&id=139&ide=55
- CONTROL DE CALIDAD (2011). Extraído el 18 de Julio de 2011 desde http://www.mundodescargas.com/apuntes-s/tecnologia/decargar_control-de-calidad.pdf

- ISO/IEC 27001 (2010). Extraído el 18 de Julio de 2011 desde http://es.wikipedia.org/wiki/ISO/IEC_27001
- NORMATIVA: ISO 27001 (2011). Extraído el 18 de Julio de 2011 desde http://www.tcpsi.com/vermas/ISO_27001.htm
- CLASIFICACIÓN DEL SOFTWARE (2011). Extraído el 18 de Julio de 2011 desde http://html.rincondelvago.com/clasificacion-del-software.htmln
- DEFINICIÓN DE APLICACIÓN (INFORMÁTICA) (2011). Extraído el 18 de Julio de 2011 desde http://www.alegsa.com.ar/Dic/aplicacion.php
- RED COMPUTADORAS (2010). Extraído el 18 de Julio de 2011 desde http://es.wikipedia.org/wiki/Red_de_computadoras
- PERALTA, Manuel. SISTEMAS DE INFORMACIÓN (2011). Extraído el 18 de Julio de 2011 desde http://www.monografias.com/trabajos14/sist-informacion/sist-informacion.shtml
- SISTEMAS DE COMUNICACIÓN (2011). Extraído el 18 de Julio de 2011 desde http://html.rincondelvago.com/sistemas-de-comunicaciones.html
- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION SEGÚN ISO 27001 (2006) Extraído el 20 de Noviembre de 2011 desde http://www.nexusasesores.com/docs/ISO27001-norma-e-implantacion-SGSI.pdf
- ESTANDAR INTERNACIONAL ISO/IEC 27001 (2005). Extraído el 20 de Noviembre de 2011 desde https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf
- CONSEJOS DE IMPLANTACIÓN Y MÉTRICAS DE ISO/IEC 27001 Y 27002 (2007). Extraído el 12 de Enero del 2012 desde http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf
- ANALISIS Y EVALUACION DEL RIESGO DE INFORMACION: APLICACIÓN DE LA ISO 27001 (2011). Extraída el 12 de Enero de 2012 desde http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf
- NTP-ISO/IEC 17799 (2007). Extraída el 2 de Febrero del 2012 desde http://www.pecert.gob.pe/media/uploads/isoiec17799.pdf

GLOSARIO DE TERMINOS

A

Access Point.- Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network) permite la conexión de los dispositivos inalámbricos a la WLAN, como: teléfonos celulares modernos, Netbook, Laptop, PDA, Notebook e inclusive otros Access Point para ampliar las redes.

Active Directory (AD).- Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (como LDAP, DNS, DHCP, etc.).

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Activo.- Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tenga valor para la organización.

Amenaza.- Según [ISO/IEC 13335-1:004]: Causa potencial de un incidente no deseado, el cual puede causar el daño al sistema o a la organización.

Análisis de riesgo.- Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Antivirus.- Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

Aplicación MRTG.- MULTI ROUTER TRAFFIC GRAPHER (MRTG) permite adquirir información del ancho de banda relacionada a las interfaces de la red en un host de red.

Archivos logs.- Un log es un registro oficial de eventos durante un rango de tiempo en particular. Es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Auditoria.- Es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones.

B

Basilea.- Se conoce al acuerdo publicado en 1988, en Basilea, Suiza, por el Comité de Basilea, compuesto por los gobernadores de los bancos centrales de Alemania, Bélgica, Canadá, España, EE. UU., Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea.

Bits de paridad.- Bit agregado a una unidad de datos, generalmente cada carácter, que sirve para comprobar que los datos se transfieran sin corrupción. El receptor revisa la paridad de cada unidad de entrada de datos

Bridge.-Es un dispositivo que conecta dos o más redes físicas que utilizan el mismo protocolo de comunicaciones y encamina paquetes de datos entre ambas.

BSI.- Instituto Británico de Normas Técnicas (BSI, British Standar Institute)

Buckup.- (Copia de seguridad) Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento.

C

Check Point.- Un punto de control, en un contexto de virtualización, es una instantánea del estado de una máquina virtual. Como un punto de restauración en sistemas operativos Windows, un puesto de control permite al administrador para devolver la máquina virtual a un estado anterior. Los puestos de control son los más comúnmente usado para crear copias de seguridad antes de realizar actualizaciones.

Cisco.- Es una marca de equipos de telecomunicaciones y redes de cómputo**.**

Confidencialidad.- Según [ISO/IEC 13335-1:2004]: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

CPU.- Central Processing Unit (unidad de proceso central), se pronuncia como La CPU es el cerebro del ordenador, es el encargado de realizar y dirigir todas las funciones.

D

Datos.- Un dato puede definirse como la unidad mínima de información o bit, puede ser un carácter una palabra.

Departamento de Sistemas.- Departamento de Tecnologías de Información de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

Discos PGP.- Para crear discos duros virtuales encriptados se usa PGP (Pretty Good Privacy). Este sistema de cifrado permite, mediante el uso de una clave pública y otra privada, mantener los datos completamente seguros mediante una encriptación de 1.024 bits (aunque es posible que este número varíe), lo que hace que sea una de las soluciones de encriptación disponibles públicamente más avanzadas en la actualidad.

Disponibilidad.- Según [ISO/IEC 13335-1:2004]: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

E

Equipo tape backup.- Es una unidad de Almacenamiento Masivo de Datos en Cinta, respuesta rápida y sencilla al problema de las Copias de Seguridad, tiene como ventaja de que el Medio Magnético (Data Cartdridge) es removible, de capacidades casi ilimitadas, confiables y duraderas. A nivel software ofrecen, además, la posibilidad de grabación de Datos en formato Comprimido, y método de corrección de Errores Avanzado.

Evaluación del riesgo.- Según [ISO/IEC Guía 73:2002]: Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información.- Según [ISO/IEC TR 18044:2004]: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

F

Firewall.- Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Freeware.- Free (gratis) + ware (software). Cualquier software que no requiere pago ni otra compensación por parte de los usuarios que los usan. Que sean gratuitos no significa que se pueda acceder a su código fuente.

Ftp.- File Transfer Protocol usado en internet, permite transferir archivos locales hacia un servidor web.

G

Gestión del riesgo.- Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

H

Hacker.- Es la persona que aprovecha sus conocimientos (experto) de la informática (redes, programación, etc.) para utilizar la vulnerabilidad de un sistema con un fin como el obtener información privada.

Hardware.- Son todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Hub.- Es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

I

IDS.- Es un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red.

Impacto.- Daño económico que se produce cuando se materializa una determinada amenaza en un activo de información.

Incidente de seguridad de la información.- Según [ISO/IEC TR 18044:2004]: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

Integridad.- Según [ISO/IEC 13335-1:2004]: la propiedad de salvaguardar la exactitud e integridad de los activos**.**

Interfaz.- Es el elemento de comunicación que facilita el intercambio de datos, como por ejemplo el teclado, que es un tipo de interface entre el usuario y la computadora.

Internet.- Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

IPS.- Es un Sistema de Prevención de Intrusos (IPS), dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

Iptable de Linux.- Es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Es decir disponible en el núcleo Linux que permite interceptar y manipular paquetes de red.

ISO.- (International Organization for Standardization - Organización Internacional para la Estandarización). Se encarga de crear estándares o normas internacionales**.**

L

LDAP.- Son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Linux.- Sistema operativo que posee un núcleo del mismo nombre. El código fuente es abierto, por lo tanto, está disponible para que cualquier persona pueda estudiarlo, usarlo, modificarlo y redistribuirlo.

M

Malware.- (del inglés malicious software), también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Mantenimiento.- Son todas las acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado en el cual pueda llevar a cabo alguna función requerida. Estas acciones incluyen la combinación de las acciones técnicas y administrativas correspondientes.

Mecanismos.- Manera de producirse o de realizar una actividad.

Medida.- Proporciona una indicación cuantitativa de la cantidad, dimensiones o tamaño de algunos atributos de un producto.

Metodología.- La metodología (meta = a través de, fin; oídos = camino, manera; lógos =teoría, razón, conocimiento): es la teoría acerca del método o del conjunto de métodos. La metodología es normativa (valora), pero también es descriptiva (expone) o comparativa (analiza). La metodología estudia también el proceder del investigador y las técnicas que emplea.

Métrica.- Medida cuantitativa del grado en que un sistema, componente o proceso posee un atributo dado.

Monitorear.- Monitorizar, observar el curso de uno o varios parámetros para detectar posibles anomalías.

O

Ocurrencia.- Evento que produce daños personales o patrimoniales a un tercero. Exposición repetida, gradual o continua, de una condición adversa, que no es ni pretendida ni esperada, con el resultado de daños personales y/o daños patrimoniales a una tercera parte.

OPENLDAP.- OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Está liberada bajo su propia licencia.

P

PDCA (planear hacer chequear actuar).- El ciclo PDCA, también conocido como "Círculo de Deming" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos. Es muy utilizado por los SGSI.

Phishing.- Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Política.- Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

Propiedad Intelectual.- Es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

R

Restricción.- Es un Límite, impedimento o limitación, en la realización de una conducta, proyecto, etc.

Revisar.- Mirar atentamente con intención de subsanar los fallos o defectos que algo pueda presentar, es decir revisar con intención de corregir datos obsoletos con sus valores actuales.

Riesgo.- Posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

Rol(es).- Papel que desempeña una persona o grupo en cualquier actividad.

Router.- También conocido como encaminador, enrutador, direccionador o ruteador— es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.

S

Seguridad de información.- Según [ISO/IEC 17799:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

Servicios.- Es un conjunto de actividades que buscan responder a una o más necesidades de un cliente. Se define un marco en donde las actividades se desarrollarán con la idea de fijar una expectativa en el resultado de éstas.

Servidor.- Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Sistema de gestión de seguridad de la información SGSI.- Esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

Shareware.- Se denomina shareware a una modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales.

SOA.- La Declaración de Aplicabilidad o Statement of Applicability (SOA) referenciado a una cláusula del estándar ISO 27001 es un documento que lista los objetivos y controles que se van a implementar en una Organización, así como las justificaciones de aquellos controles que no van a ser implementados.

Software blade de Check Point.- Arquitectura de seguridad que consiste en una combinación de funciones de seguridad basadas en un Gateway de Seguridad de

Check Point o un Sistema de Management, con la garantía que todas estas aplicaciones son interoperables y pueden brindar un nivel de performance predecible.

Spyware.- El spyware o programa espía es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Switch.- El switch (palabra que significa "conmutador") es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria.

T

Tasación.- o valoración es el proceso de estimar el valor de un activo.

Tercero.- Cualquier persona física o de existencia ideal que no es ni titular, ni procesador, ni responsable de un banco de datos, ni agente o empleado de estos últimos.

Tecnología RAID5.- Es un sistema de almacenamiento el cual hace uso de múltiples discos entre los cuales replica los datos, este se aplica bajo un escenario regularmente de servidores en el cual se poseen como mínimo 3 unidades de discos duros y se desea tener la división de datos a nivel de bloques distribuyendo la información de paridad entre todos los miembros del sistema de RAID, por lo tanto, un sistema RAID 5 proporciona beneficios como una mayor integridad, mayor tolerancia a fallos, mayor rendimiento, mayor fiabilidad y sobre todo mayor capacidad.

Tratamiento del riesgo: Según [ISO/IEC Guía 73:2002]: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo

NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

Trialware.- Demoware (también conocido como trialware) es un tipo de software que permite su uso sin ninguna restricción por un período limitado de tiempo. Pasado ese tiempo, se deshabilitan ciertas funciones.

U

Ups.- Es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

V

Validación.- Es el proceso de comprobar la precisión de los datos; conjunto de reglas que se pueden aplicar a un control para especificar el tipo y el intervalo de datos que los usuarios pueden especificar.

Valuación del riesgo.- Según [ISO/IEC Guía 73:2002]: Proceso general de análisis del riesgo y evaluación del riesgo.

Validez jurídica.- Se designa, como válida una norma cuando cumple con los requisitos formales y materiales necesarios para su producción. La validez de la norma no depende sólo del acto de su promulgación y publicación, a partir del cual se declara la existencia de la norma, aunque si es uno de sus efectos, en tanto la norma debe existir jurídicamente para poder ser exigible.

Virus Informático.- Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

VPNS (clientes móviles).- (Virtual Private Network) Red privada virtual. Red de comunicaciones de área ancha provista por una portadora común que suministra aquello que asemeja líneas dedicadas cuando se utilizan, pero las troncales de base se comparten entre todos los clientes como en una red pública

Vulnerabilidad.- Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

W

Web service.- Es una pieza de software que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

ANEXOS

ANEXO 1

Plan de capacitación y conocimiento para el personal del departamento de sistemas

El Departamento De Sistemas del Cooperativa de Ahorro y Crédito "San Francisco" Ltda. , es un sector muy importante para el desarrollo óptimo y efectivo de las tareas diarias, debido principalmente al uso generalizado de equipos de computación, soluciones de software, equipos de intercomunicación y redes, tanto a nivel local como a nivel metropolitano.

I. JUSTIFICACIÓN

Debido a un estudio realizado en el departamento sobre la adopción de un Sistema de Gestión de Seguridad de la Información, ya que es muy importante para mantener y mejorar la confiabilidad, integridad y disponibilidad de los sistemas de información y comunicación, se ve la necesidad de dar a conocer al grupo de trabajo del departamento de sistemas sobre la aplicabilidad del sistema de gestión y así elevar y mantener la seguridad en todo el departamento de sistemas mejorando los servicios brindados del departamento juntamente con toda la Cooperativa.

II. ALCANCE

El presente plan de capacitación es de aplicación para todo el personal que trabaja en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito "San Francisco" Ltda.

III. OBJETIVOS DEL PLAN DE CAPACITACION

Objetivos Generales

- Preparar al personal para operar, mantener y mejorar el sistema de gestión de seguridad de la información.

Objetivos Específicos

- Proporcionar orientación e información relativa a los objetivos del sistema de Gestión de Seguridad de la Información.
- Proveer conocimientos y desarrollar habilidades que cubran la totalidad de la operatividad del Sistema de Gestión de Seguridad de la Información.
- Contribuir a elevar y mantener un buen nivel de eficiencia individual y rendimiento colectivo en cuanto a la seguridad informática.

IV. ESTRATEGIAS

Las estrategias a emplear son:

- Desarrollo de trabajos prácticos para comprender con exactitud el sistema de gestión de seguridad de la información
- Presentación de casos particulares del área, que ayudaran a mejorar la operatividad del Sistema de Gestión de Seguridad de la Información.

V. MODALIDAD DE CAPACITACION

El propósito de esta capacitación es impartir conocimientos básicos orientados a proporcionar una visión general y amplia con relación al contexto del sistema de Gestión de Seguridad de la Información.

Se realizara 5 reuniones de dos horas diarias a partir de las 18:30 el personal destinado para esta capacitación son los trabajadores del departamento de sistemas.

VI. TEMAS DE CAPACITACIÓN

Sistema de Gestión de Seguridad de La Información

VII. RECURSOS

HUMANOS.- Lo conforman las personas que laboran en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “San Francisco” Ltda.

ANEXO 2

ENTREVISTA

OBJETIVO: Recolectar información para determinar las condiciones de seguridad en las que se encuentra los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito "SAN FRANCISCO" Ltda.

Nombre:……

Función que desempeña:……

Telf.:……. e-mail:……

1. **¿Se aplican políticas de seguridad para la información. SI…. Enúncielas; NO….Porque?**

……
……
……
……

2. **¿De qué manera se realiza un control de la seguridad de la información?**

……
……
……
……

3. **¿Describa el control interno informático que se realiza en el Departamento de Sistemas?**

……
……
……
……

4. ¿**Conoce usted acerca de un Sistema de Gestión de seguridad de la Información (SGSI)?**

……
……
……
……

5. **¿Cómo se garantiza la confiabilidad, integridad y disponibilidad de la información que se procesa en los sistemas de información y de comunicación?**

   ……
   ……
   ……
   ……

6. **¿Qué mecanismos, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y comunicación?**

   ……
   ……
   ……
   ……

7. **¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?**

   ……
   ……
   ……
   ……
   ……

8. **¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?**

   ……
   ……
   ……
   ……

9. **¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación. Si……De qué manera se lo ha realizado; No…..Porque?**

   ……
   ……
   ……
   ……