UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

ARTÍCULO CIENTÍFICO

TEMA:

"PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002"

AUTOR: DONY ANDERSON REINA LÓPEZ

DIRECTOR: MSC. JAIME MICHILENA

IBARRA – ECUADOR

2017

Pan de contigencia para la Cooperativa de Ahorro y Crédito de Indigenas Chuchuqui Ltda., basado en la norma ISO/IEC 27002

Autores – Dony Anderson REINA LÓPEZ, Ing Jaime Roberto MICHILENA CALDERÓN, MSc.
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Avenida 17 de Julio 5-21 y José María Córdova, Ibarra, Imbabura
jlortiza@utn.edu.ec, jrmichilena@utn.edu.ec

Resumen— Este proyecto se trata de un Plan de Contingencia que tiene su aplicación en la COAC Chuchuqui Ltda. de la ciudad de Otavalo. Para su desarrollo se revisaron las normas internacionales descritas por la unión técnica de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), así como también publicaciones de ITIL (Librería de Infraestructura de Tecnologías de la Información), para tomar un modelo base normalizado y de buenas prácticas que esté relacionado a la seguridad de la información.

En este trabajo se contempló un análisis de riesgos, un plan de emergencia, un plan de restauración, un plan de recuperación, pruebas y evaluación y un plan de mantenimiento, lo cual permitió establecer parámetros sobre los cuales fue necesario la implementación de controles de seguridad.

También dentro de la implementación de controles de seguridad se montó un sistema de monitoreo para los servidores del centro de datos de la COAC en una plataforma de software libre (NAGIOS), se realizó un escaneo de puertos abiertos en la red y las precauciones que se deben tomar para estos, se mejoró la seguridad física de los equipos mediante la implementación de una lectora de huellas para el control de acceso al Data Center al igual que una puerta de seguridad y un sistema de aire acondicionado.

Se realizó una capacitación del personal de la cooperativa sobre la seguridad de la información, lo que ayudó a mejorar los principios de seguridad (confiabilidad, integridad y disponibilidad), también se dio a conocer las nuevas políticas de seguridad instauradas en el último trimestre del año 2016 y una guía de cómo realizar la clasificación de la información.

I. INTRODUCCIÓN

La Cooperativa de ahorro y crédito CHUCHUQUI como institución financiera tiene el compromiso con la sociedad de brindar a sus socios productos y servicios financieros de calidad, generando un crecimiento y rentabilidad sostenida. Uno de los requerimientos para cumplir con este compromiso es el mantener segura la red de información, generando estrategias que ayuden a subsanar los hallazgos identificados en la auditoría realizada por la SEPS según lo expresa el oficio circular N°SEPS-IFPS-2014-03570 del 26 de febrero de 2014.

Debido a las exigencias de la SEPS después de revisar los informes de auditorías como se manifiesta en el Reglamento de la Ley Orgánica de la Economía Popular y Solidaria en el Art. 154 y dada la importancia de la información que maneja diariamente la cooperativa es fundamental la implementación de mecanismos de seguridad en redes, que protejan los datos que se transmiten e interactúan en la red de datos. Implantando recursos de protección para que no se violen las barreras de acceso al Data Center y la información que en ellos se maneja o almacena, que puedan generar pérdidas a la cooperativa.

Es necesario que la entidad intente alcanzar que la SEPS certifique que la cooperativa cuenta con una continuidad de negocio respecto a la tecnología de información y la realización de un plan de contingencia respalda que la cooperativa se encuentre en una etapa de crecimiento tecnológico. Además de proporcionar servicios de calidad para garantizar un mayor nivel de confiabilidad en sus socios y clientes.

Cuando se tiene una transferencia de datos con altos niveles de seguridad informática le permite al beneficiario reducir costos operativos, mejorar su viabilidad, escalabilidad y costo-beneficio de la estructura de la red, obteniendo una gran ventaja para sobresalir en la competitividad con otras entidades del mismo carácter.

II. ORGANISMOS REGULADORES

NORMA TÉCNICA ISO/IEC 27002

La norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar una gestión de seguridad de la información en una organización. Los objetivos definidos en esta norma proveen directrices generales sobre las metas generadas para una gestión de la seguridad de la información.

Los objetivos de los controles de esta norma, tienen como finalidad ser puestos en marcha para socorrer a los requisitos generados por medio del análisis y evaluación de los riesgos. Esta norma

puede servir como guía práctica para desplegar los procedimientos de seguridad de la información de la institución y las eficientes prácticas de gestión de seguridad, y para generar una creciente confianza en las actividades que envuelven a los clientes.

Esta norma cuenta con 14 dominios de seguridad de la información que juntas totalizan 35 categorías principales y 114 controles de seguridad, además de una introducción de análisis y evaluación para el tratamiento de riesgos.

Dominios.

Cada dominio cuenta con un número de categorías principales de la seguridad de la información. Los 14 dominios son (los números en los paréntesis representan la cantidad de categorías para cada dominio los cuáles se detallan en el Plan de Mantenimiento):

- Política de seguridad de la información (1)
- Aspectos organizativos de la seguridad de la información (2)
- Seguridad ligada a los recursos humanos (3)
- Gestión de activos (3)
- Control de Accesos (4)
- Cifrado (1)
- Seguridad física y ambiental (2)
- Seguridad en la operativa (7)
- Seguridad en las telecomunicaciones (2)
- Adquisición, Desarrollo y Mantenimiento de sistemas de información (3)
- Relaciones con suministradores (2)
- Gestión de incidentes de seguridad de la información (1)
- Aspectos de la seguridad de la información en la gestión de continuidad del negocio (2)
- Cumplimiento (2)

Nota: *el orden de los dominios en esta norma no significa su grado de importancia. Dependiendo de las circunstancias, todas las secciones pueden ser importantes. Por lo tanto, conviene que cada organización que utilice esta norma identifique cuáles son los ítems aplicables, que importancia les dan y sus aplicaciones para los procesos específicos de negocio. Todas las alineaciones en esta norma no están ordenadas por prioridades a no ser que se indique.*

NORMA TÉCNICA NTC/ISO 27005:2005

Esta norma está desarrollada gracias a la participación de la ISO (Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) que en sí son las que forman el sistema especializado a nivel mundial para la normalización. además de estos existen otros organismos que conforman comités para tratar temas técnicos. Cuando el comité técnico de estos organismos superiores da a conocer una nueva Norma Internacional a todas las organizaciones nacionales, debe cumplir con el 75% de aprobación realizando una votación.

La NTC-ISO 27005, proporciona guías o directrices que dan soporte a la gestión del riesgo en la seguridad de la información para una institución, cubriendo los requisitos que conlleva un sistema de gestión de seguridad de la información (SGSI) en relación a la norma ISO 27001.

Esta norma sirve como apoyo para la implementación satisfactoria de los controles generales descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 para la seguridad de la información, con su enfoque en la gestión de riesgos, por lo cual es necesario tener conocimientos previos de estas dos normas. Esta norma aplica para cualquier organización que tenga en bien el análisis de riesgos para cubrir las necesidades de la seguridad informática.

ITIL V3

ITIL (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) es un extracto de publicaciones, o libros en sí, que describen de manera sistemática un conjunto de “buenas prácticas” para la gestión de los servicios de Tecnología Informática.

En vista de que las instituciones cada vez dependen más de las tecnologías de información para el desarrollo de sus actividades diarias, así como también para su control y gestión a través de sistemas de información, y que todo esto a su vez se encuentra dentro de una red que puede estar controlada por otros sistemas informáticos. Por lo tanto, al ver toda esta complejidad que se contiene en las redes y sistemas informáticos, lleva a varias instituciones a recurrir a la necesidad de contar con un modelo de gestión para todo lo que conforma la infraestructura de TI, que sea eficaz y de fácil implementación.

Es así, como en la década de los 80 nació ITIL por medio de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency – CCTA), que pensó e implantó una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costes derivados de los recursos TI. En la actualidad ITIL pertenece al Oficina de Comercio Británico (Office of Government Commerce – OGC), pero puede ser utilizado para su aplicación libremente.

ITIL descubrió la necesidad de realizar un estudio que contenga una agrupación de libros según conjuntos estructurados en los procesos que estuviesen más relacionados, enmarcando la gran cantidad de publicaciones existente en ocho volúmenes, denominándose desde entonces como ITIL v2.

Su última versión fue publicada en el año 2007, tildada como ITIL v3. En esta versión se ha realizado un renuevo de la información ya publicada, que agrupa los principales elementos de ITIL en 5 volúmenes, que pueden encontrarse en la actualidad con los siguientes títulos (en inglés original):

- ITIL v3 Service Strategy (SS)
- ITIL v3 Service Design (SD)
- ITIL v3 Service Operation (SO)
- ITIL v3 Continual Service Improvement (CST)
- ITIL v3 Service Transition (ST)

COBIT

COBIT (Control Objetives for information and related Technology, Objetivos de Control para Tecnologías de información y relacionadas) es un conjunto de buenas prácticas para la gestión de la información creado por ISACA (Information Systems Audit and Control Association, Asociación para la Auditoría y Control de sistemas de información) con el apoyo del Instituto de Administración de las Tecnologías de la Información (IT Governance Institute), en el año 1992.

COBIT fue creado con la finalidad de proporcionar una guía que garantice el control y gestión adecuados de las tecnologías de la información, con el objetivo de alcanzar los objetivos del plan de negocio de cualquier organización. Por lo tanto, COBIT es un soporte de apoyo para las instituciones que abarca un conjunto de herramientas que permiten a los administradores cubrir los requerimientos de control, cuestiones técnicas y los riesgos del negocio dentro de todos los niveles de la organización y partes interesadas.

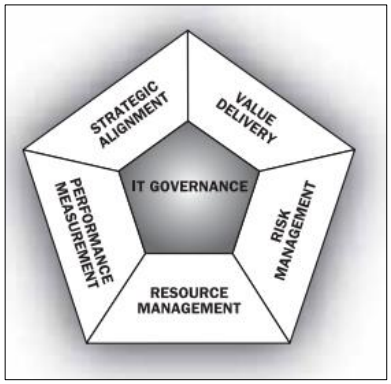

Figura 1: Áreas de enfoque de COBIT

Fuente: IT Governance Institute (2007). COBIT (Control Objetives for information and related Technology). Rolling Meadows: Algonquin Road.

COBIT proporciona un marco referencial de soporte que podemos observar en la Figura 1, que garantiza:

- TI está alineada con el negocio
- Permite que el negocio maximice los beneficios de TI
- Los recursos de TI se utilizan de forma responsable
- Los riesgos de TI se manejen de forma adecuada

III. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA.

ACTIVOS DE INFORMACIÓN

En la actualidad para toda institución, la información ha pasado a ser el activo con el valor más significativo, por lo cual deben existir varias metodologías para su adecuado almacenamiento y protección. La información de una organización se la puede encontrar en distintas maneras, puede ser documentos impresos, en unidades digitales de almacenamiento, discos extraíbles, en bases de datos de los servidores etc.

Con la finalidad de evitar pérdidas es necesario contar con controles de seguridad, que garanticen los principios de la información (confiabilidad, integridad y disponibilidad). La COAC no cuenta con todos los controles necesarios que certifiquen que la información se encuentra segura, por ejemplo, en la Figura 2 se observa la falta de gabinetes para los equipos de conexión intermedia. Se ha realizado un análisis de los controles, basándose en la norma técnica ISO/IEC 27002, el cual se encuentra detallado en el punto referente al análisis FODA.

Figura 2: Equipos de conexión intermedia sin protección.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Con la ayuda del análisis FODA se puede tratar de cubrir los aspectos negativos para la seguridad de la información, sabiendo aprovechar los controles ya existentes, por ejemplo, los discos extraíbles, discos duros y backups de la COAC se encuentran protegidos en la bóveda de la institución, ya que este es el lugar más seguro.

RED DE DATOS

La COAC Chuchuqui cuenta con una red de datos interna de cableada hacia los distintos departamentos que la conforman, y una inalámbrica únicamente para dispositivos autorizados por el Departamento de Tecnología, el enlace es de 6 Mbps. En Tabla 1 se encuentra una descripción de las redes de comunicación.

Tabla 1. Redes de comunicación de la COAC Chuchuqui.

RED	DESCRIPCIÓN
Red Local	Está conformada por la red cableada categoría 5e.
Red Wireless	Está conformada por la red inalámbrica distribuida exclusivamente para la 2da planta alta y la 3ra planta alta.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

La topología de red no se encuentra establecida adecuadamente, incluso es difícil deducir el tipo de topología que está empleando, debido a que no existe etiquetado, la distribución hacia las diferentes plantas de la institución no es adecuada ya que no posee un switch de distribución para cada piso como se muestra en la Figura 3 Topología de red de la COAC Chuchuqui Ltda. El proveedor del servicio de internet es CNT EP, que suministra mediante fibra óptica monomodo de 6 hilos.

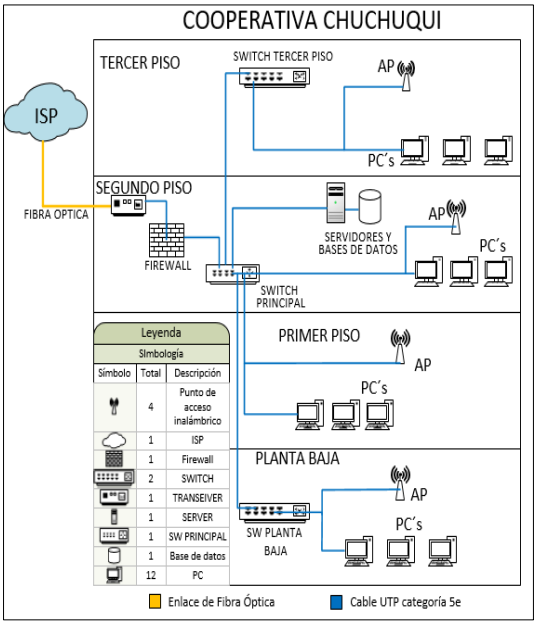

Figura 3: Topología de red de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

La estructura de red y el cableado estructurado lleva varios años sin ser modificado ni renovado, por lo cual existe la necesidad de establecer una nueva topología de red que garantice la seguridad de la información, considerando las diferentes normas de cableado estructurado.

La norma ANSI/EIA/TIA 569 C nos habla sobre el espaciado para el manejo de equipos y es una característica que no se ha tomado en cuenta en la distribución de los equipos en la COAC Chuchuqui Ltda., esta norma nos especifica que se debe proporcionar un espacio libre posterior de 0,6 m (2 pies) para el acceso de servicio en la parte posterior de bastidores y gabinetes, pero es mayormente recomendable tener un espacio posterior de 1 m (3 pies) para mejor manejo de dispositivos.

Otra norma con la que no cumple la COAC Chuchuqui es la ANSI/EIA/TIA 568 C.1-1 la cual especifica como diseñar un sistema de cableado de telecomunicaciones para edificios comerciales, además de los espacios que se deben manejar en áreas de trabajo también se muestra la forma de planificar, distribuir espacios e instalar medios de transmisión

CUARTO DE TELECOMUNICACIONES

El área del Data Center se encuentra ubicado en la 2da planta alta de la COAC y es de 9m2. Está conformado por un gabinete de piso donde se alojan los equipos de networking, 4 servidores tipo torre, 1 servidor tipo rack y una central telefónica analógica Panasonic, también contiene un UPS de 6KVA no administrable, 1 servidor tipo PC fuera del gabinete y un sistema de protección eléctrica.

El Data Center carece de un sistema de aire acondicionado, por lo que las temperaturas del cuarto son elevadas, también carece de una puerta de seguridad y un biométrico para acceso sólo a personas autorizadas, como se puede observar en la Figura 4. En este cuarto también existe una ventana, lo cual no es recomendable para un Data Center, en la Figura 5 se muestra la ventana vista desde el interior del Data Center.

Figura 4: Puerta de Acceso al Data Center

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 5: Ventana en el interior del Data Center de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Además, el Data Center debe mejorar en aspectos de la alimentación de energía eléctrica como se muestra en la Figura 6, también en la pintura empleada en las paredes e incrementar rótulos informativos de seguridad industrial.

Figura 6: Fuente de alimentación para equipos en el Data Center de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

IV. DESARROLLO DEL PLAN DE CONTINGENCIA

ESTRUCTURA

En la Figura 7, se puede observar las etapas en las que se encuentra dividido el Plan de Contingencia.

Figura 7: Etapas del Plan de Contingencia

Fuente: Elaboración propia.

- Análisis de riesgos

Antes de que suceda una eventualidad, cualquier institución debe tratar de mitigar los impactos mediante un análisis de riesgos, este procedimiento es indispensable para empezar a desarrollar un Plan de Contingencia y tener una idea de cómo enfrentarse a un incidente.

En este punto se analizarán los riesgos de un impacto y dependiendo de estos se otorgará un nivel de prioridad y se establecerá que tipo de sub-plan es el más adecuado para ponerlo en marcha.

En la Tabla 2 se puede observar una descripción de los cuatro sub-planes contenidos en el Plan de Contingencia, los cuales se accionarán dependiendo del tipo de eventualidad y estimación de riesgos.

- Pruebas de verificación y evaluación:

Antes de que un Plan de Contingencia sea aprobado por un consejo directivo, éste debe ser sometido a una serie de pruebas, para comprobar que los procedimientos propuestos en dicho plan, obtengan los resultados esperados, para ello el personal debe estar entrenado en los distintos escenarios de prueba. Al final se realizará un análisis de los resultados y se determinará si el Plan es el adecuado para la institución.

Tabla 2: Sub-planes de Contingencia

	EMERGENCIA	**RESTAURACIÓN**	**RECUPERACIÓN**	**MANTENIMIENTO**
OBJETIVO	Limitar los daños	Continuar procesos	Recuperación total de los procesos	Prevenir daños
ACTUACIÓN	Inmediata	Inmediata	A corto plazo	Continuamente
CONTENIDO	Evacuación y evaluación de daños	Alternativas para los procesos significativos	Estrategias para la recuperación de todos los recursos	Reglamentos, normas, políticas de seguridad

RESPONSABILIDAD PRINCIPAL	Usuarios y empleados de la cooperativa	Departamento de Tecnología y WEBCOOP	Departamento de Tecnología	Usuarios y empleados de la cooperativa

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

ANÁLISIS DE RIESGOS

Identificación del riesgo.

El propósito principal de la identificación del riesgo es que cualquier organización esté en la capacidad de poder anticiparse a lo que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos que se van a desarrollar a continuación, deberían ayudar a recolectar datos de entrada para la actividad de estimación del riesgo. En la Figura 8 se puede observar los porcentajes de distintos tipos de riesgos a los que se encuentran expuestos los sistemas de información.

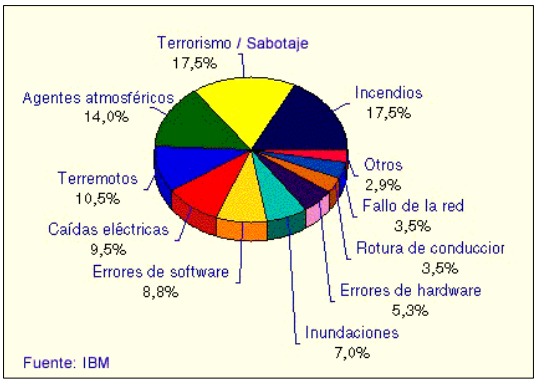

Figura 8: Riesgo a los cuales se encuentran inmersos los Sistemas de Información

Fuente: Sánchez A. (2012). Resguardar Información: Clasificación de respaldos de la información. Recuperado el 24 de noviembre de 2016 de: http://azaleasanchez-resguardarinformacion.blogspot.com/2012/02/clasificacion-de-respaldos-de-la.html

Identificación del impacto.

Un impacto puede ser la considerado como pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc. Este proceso permite establecer los daños o consecuencias que sufre una organización y que son causados por lo que esta norma lo denomina como un escenario de incidente. Un escenario de incidente se genera a partir de los detalles de una amenaza, la cual puede aprovechar una vulnerabilidad determinada o en algunos casos, un conjunto de vulnerabilidades de una eventualidad en la seguridad de la información (ISO/IEC 27002, 2013).

Para el establecimiento del impacto de los escenarios de incidentes se toma en consideración los criterios del impacto que deben ser definidos en la determinación del contexto o, en otras palabras, se debe identificar las causas de estos escenarios. Es necesario que se identifique activos o sistemas se ven afectados en cada escenario. De esta manera, poder determinar el valor de esos activos y los costos financieros a los que se ve sometida la institución.

Estimación del riesgo.

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes.

La evaluación y administración de estos riesgos van a permitir a la Cooperativa:

- Desarrollar estrategias de recuperación y respaldo de las decisiones operacionales, tecnológicas y humanas.
- Identificar los controles existentes y los nuevos controles a implementar para minimizar los riesgos, evaluando el costo / beneficio de dichos controles.
- Planificar la seguridad de la información.

Para una correcta estimación de los riesgos es necesario identificar los procesos más importantes, los servicios principales a ser reestablecidos, y la información que debe ser respaldada dentro de la institución, y dependiendo de esta importancia determinar la estimación o criticidad del riesgo.

Principales Procesos Identificados

Software

- WEBCOOP “Sistema Corporativo Web”
- SADFIN “Sistema de Administración financiera y contabilidad”
- ZENTYAL “Administrador de correos, active directory, internet, webserver, firewall, servidor de archivos, etc.”

Principales servicios que deberán ser restablecidos y/o recuperados

- Windows (PC CLIENTE)
  - Internet.
  - Herramientas de Microsoft Office.
- Software Base (SERVIDOR)
  - Base de MySQL Server
- Respaldo de la Información (SERVIDOR)
  - Backup de la configuración de CENTOS 5
  - Backup de la Base de Datos de WEBCOOP (SQL)
  - Backup de la WEBSITE

- Backup del Servidor SADFIN.

En la Tabla 3, se mencionan los tipos de impactos que pueden causar los riesgos con su descripción y valoración asignada. Esto es necesario para saber que prioridad se da al riesgo al proponer una solución.

Tabla 3. Tipos de Impactos de los Riesgos

Impacto	Valor	Descripción
Crítico	4	Pérdida de la información confidencial y cuando ocurren daños significativos en los equipos.
Alto	3	Cuando se ven afectadas las operaciones y funciones, información de los usuarios y sistemas de información institucional
Medio	2	Cuando los daños son parciales (solo se dan en ciertos sistemas sin afectar las operaciones)
Bajo	1	Cuando no afectan las actividades ni los sistemas principales

Fuente: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Así, como los tipos de impactos es importante describir los tipos de frecuencia en la que los riesgos pueden ocurrir. En la Tabla 4 se indica el tipo de frecuencia de ocurrencia de una amenaza.

Tabla 4. Tipos de Frecuencia de ocurrencia de una amenaza.

Frecuencia	Valor	Descripción
Crítico	5	Cuando un riesgo o amenaza sucede de una a tres veces al día
Alto	4	Cuando un riesgo o amenaza sucede de una a tres veces a la semana
Medio	3	Cuando un riesgo o amenaza sucede de una a tres veces al mes
Bajo	2	Cuando un riesgo o amenaza sucede de una a tres veces al año
Poco Probable	1	Su valor es bajo ya que es casi improbable que pase o pueda que ocurra una sola vez cada tres años o más.

Fuente: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Una vez establecido los tipos de impactos y tipos de frecuencia podemos establecer la estimación de los riesgos mediante la metodología MAGERIT, que compara el valor del Impacto y de la Frecuencia, como se indica en la Tabla 5.

Tabla 5. Estimación del riesgo según análisis MAGERIT.

RIESGO		FRECUENCIA				
		Crítica	Alta	Medio	Baja	Poco Probable
IMPACTO	Crítico					
	Alto					
	Medio					
	Bajo					

Fuente: Elaboración propia.

Análisis FODA

Este análisis se ha visto como una evolución dentro de los sistemas de gestión y planificación y a formado parte de los aspectos más importantes de las empresas para la supervivencia y adaptación a nuevos cambios.

De este análisis se derivan dos aspectos: externos e internos los cuales se encuentran agrupados bajos los siguientes conceptos:

- Aspectos externos. Su análisis se realiza en base a la relación que estos tienen con el ambiente al que se encuentran expuestos o el estado actual en el que se encuentran y los cambios que se espera que tengan en un futuro, tomando en cuenta que, por lo general, estos aspectos no son controlables. Dentro de estos aspectos se encuentran los conceptos de oportunidades y amenazas.

- Aspectos internos. Su análisis se realiza en base al estado actual en el que estos se encuentran y las variables en análisis que estos necesitan para mantener la competitividad de toda la institución en general. Ya que según expertos los aspectos internos son los que establecen la sostenibilidad de la competitividad. Dentro de estos aspectos se encuentran los conceptos de fortalezas y debilidades.

A continuación, en la Figura 9 se muestra un resumen de los objetivos y controles de la norma ISO/IEC 27002 en los cuales se basa este análisis FODA. Para este resumen se eliminaron algunos controles de seguridad, que no se aplican para la COAC CHUCHUQUI, ya que no se encuentran relacionadas con las actividades que en ella se desarrollan.

Para este análisis se ha tomado en cuenta la norma ISO/IEC 27002:2013 de la cual se ha analizado cada uno de los objetivos y controles en relación a la situación actual en la que se encuentra la COAC (Cooperativa de Ahorro y Crédito), y clasificando cada uno respecto a los conceptos de esta metodología. En la Tabla 6 se muestra cada descripción que viene acompañada del literal de la norma al cual se encuentra relacionada.

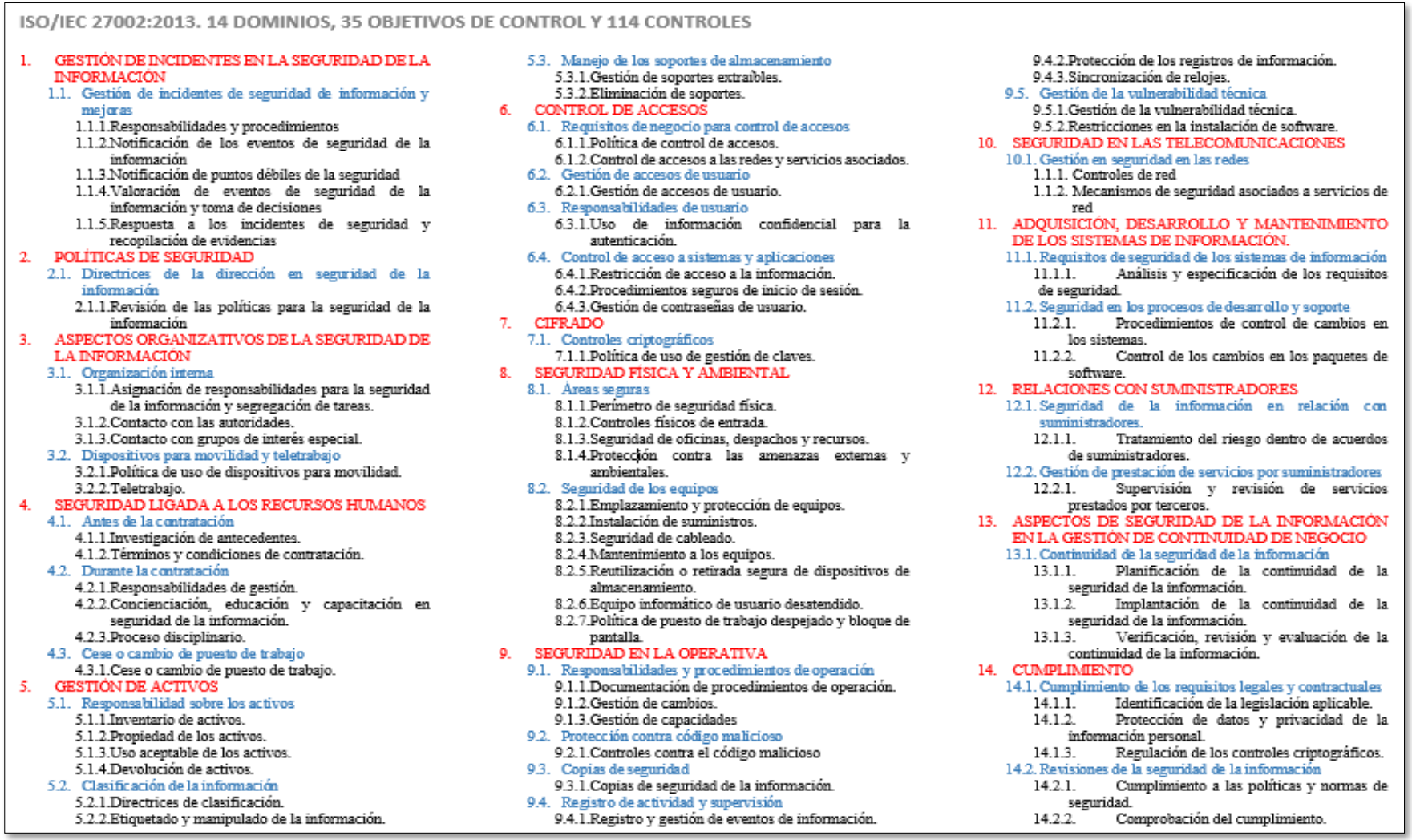

Figura 9: Resumen norma ISO/IEC 27002:2013

Fuente: Acoplado de ISO/IEC 27002:2013

Tabla 6. Resultado Análisis FODA

F (Fortalezas)	O (Oportunidades)	D (Debilidades)	A (Amenazas)
Políticas de movilidad y teletrabajo no establecidas. (3.2) Contratos establecen puntos de confidencialidad y responsabilidades. (4.1.2) Cuenta con Políticas de control de acceso. (6.1) Se exige el uso de buenas prácticas de seguridad en la organización. (6.3) Control de acceso a sistemas y aplicaciones. (6.4) Gestión de claves. (7) Se encuentran bien definidas las áreas de acceso al público. (8.1) Los equipos activos como servidores y bases de datos, se encuentran protegidos y aislados de personas no autorizadas. (8.2.1) Existen procedimientos de información puesta a disposición de los usuarios. (9.1.1) Se trata de ejecutar un mínimo de cambios posibles en la seguridad de la información, que puedan tener alguna afectación en la información. Los cambios que se realizan es bajo supervisión. (9.1.2) Los servidores se encuentran bajo monitoreo y los recursos de red están correctamente distribuidos mediante reglas de acceso. (9.1.3) Todos los dispositivos Móviles (Laptops) conectados a la red cuentan con antivirus licenciado. (9.2) Se realizan copias de seguridad de la información ni respaldos de las bases de datos. (9.3) Se controla el registro de actividad del administrador y operador del sistema. (9.4.1) Todos los sistemas se encuentran sincronizados. (9.4.3) Existe restricción respecto a la instalación de software. (9.6.2) Están establecidas medidas de seguridad en las telecomunicaciones. (10) Se realiza periódicamente una revisión técnica de las aplicaciones tras efectuar cambios en los sistemas operativos. (11.2.1) Existe restricción a los cambios en los paquetes de software. (11.2.2)	Creación paulatina de políticas de seguridad. (1.1) Existen directrices de clasificación de la información, pero no han puesto en marcha. (5.2) Cuenta con sistemas de Detección de incendios y extintores para extinción de incendios. (8.1.3) Cuenta con UPS y generados de energía de iniciación manual. (8.2.2) Falta adaptar adecuadamente la política de puesto de trabajo despejado y bloqueo de pantalla. (8.2.7) Se está desarrollando un análisis y especificación de los requisitos de seguridad. (11.1.1) Se aplica el uso de principios de ingeniería en protección de sistemas. (11.2) Se está desarrollando la gestión de incidentes en la seguridad de la información. (1) Conocimiento de las políticas que establecen los proveedores de servicios acerca de la seguridad de la información. (12)	Los funcionarios pertenecientes al departamento de tecnología no tienen asignadas responsabilidades y procedimientos relacionados con la seguridad de la información. (1.1.1) y (3.1.1) No existe un modelo para la valoración de eventos de la seguridad de la información y toma de decisiones. (1.1.4) Aún no se define los contactos de interés y gestión de la seguridad de la información. (3.1) No se realiza capacitaciones continuas sobre la seguridad de la información. (4.2.2) Posee un registro de los equipos activos de red, pero se encuentra desactualizado. (5.1) No existe etiquetado y manipulado para la información. (5.2.2) Falta mejor aspectos de Seguridad en oficinas específicamente no existe señalética adecuada en todos los sectores de la institución. (8.1.3) La protección contra amenazas externas y ambientales se encuentra sujeta a la construcción arquitectónica actual. (8.1.4) Los funcionarios carecen de la costumbre para la aplicación de la política de puedto de trabajo despejado. (8.2.7) No existe un control para la gestión de cambios. (9.1.2) No existe IDS e IPS de detección y prevención para el control de código malicioso. (9.2) No se han realizado periódicamente controles de auditorías de los sistemas de información. (9.5) No existe gestión de las vulnerabilidades técnicas. (9.5.2) No se realiza periódicamente una verificación, revisión y evaluación de la continuidad de la información. (13.1.3) No se realizan comprobaciones periódicas del cumplimiento de las políticas y normas de seguridad. (14.2)	Acceso por SSH habilitado y se maneja el puerto por defecto. (11.1) Equipos de interconexión que se encuentran fuera del Data Center están accesibles. (5.3) No cuentan con sistema de gestión de acceso de usuario, derechos de acceso y de privilegios especiales. (6.2) Los equipos de interconexión se encuentran desprotegidos ante intercepción, interferencia y posibles daños. Y el cableado estructurado necesita do en varios sectores. (8.2.3) Carece de una política que permita y restrinja la reutilización o restricción segura de dispositivos de almacenamiento. (8.2.5) No se toman las medidas necesarias para la supervisión y revisión de servicios prestados por terceros. (12.2.1)

Fuente: Elaboración propia.

PLAN DE EMERGENCIA

Estimación de escenarios.

La estimación de los escenarios de incidentes nos permite determinar los instrumentos necesarios para poder dar priorización y orientación las acciones que van a llevarse a cabo cuando suceda alguno de estos incidentes. Así, como también corregir vulnerabilidades y de esta forma obtener mejores resultados en la prevención y en el proceso de mitigación de los riesgos. En la Tabla 7 podemos ver ejemplos de riesgos de emergencia con sus respectivas medidas y tiempo de implementación.

Tabla 7. Ejemplos de riesgos de emergencia

RIESGO	MEDIDA A IMPLEMENTAR	TIEMPO DE IMPLEMENTACIÓN
Sismo de 6.5° en la escala de Richter, de origen tectónico.	Realización de simulacros de evacuación, para el personal que labora en la cooperativa. Verificación del funcionamiento de alarmas. Comprobación de que no exista estanterías o cuadros no susceptibles a caídas.	Mediano plazo: de 6 a 9 meses.
Incendio	Evaluación de las instalaciones eléctricas para garantizar la reducción de la probabilidad de un cortocircuito.	Corto plazo: de 3 a 6 meses
Aparatos explosivos	Capacitación del personal de seguridad, con la finalidad de establecer medidas de protección en caso de encontrar paquetes sospechosos en las instalaciones de la institución.	Mediano plazo: de 6 a 9 meses.

Fuente: Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de: http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Organización institucional de respuesta.

La institución debe establecer una organización o comité institucional de respuesta, el cual será responsable de dirigir el proceso de ejecución del plan de emergencia. A continuación, en la Figura 10 se describe gráficamente la estructura:

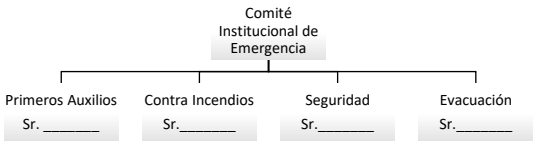

Figura 10. Comité Institucional de Emergencia

Fuente: Elaboración propia.

PLAN DE RESTAURACIÓN

Para el desarrollo del plan de restauración se deberá tomar en cuenta la Figura 11, en la que expone un diagrama de flujo que propone una estructura de procedimiento de gestión de incidentes basado en ITIL.

Figura 11: Procedimiento de Gestión de Incidencias

Fuente: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

Los tiempos de restauración se basan en la publicación de ITIL, la cual también propone un sistema de código de prioridad como se muestra en la Tabla 8.

Tabla 8. Clasificación de tiempos de restauración

Código de prioridad	Descripción	Tiempo objetivo de restauración
1	Crítico	1 hora
2	Alto	8 horas
3	Medio	24 horas
4	Bajo	48 horas

Fuente: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

Hay que tomar en cuenta que el impacto, prioridad y tiempo, pueden variar a lo largo del análisis de la incidencia como se describe a continuación:

- Puede ampliarse debido al aumento de los fallos o al tratarse de una secuencia de fallos.
- Puede reducirse al implementar soluciones temporales que sean eficaces de tal manera que se dé por terminado el incidente.

PLAN DE MANTENIMIENTO

Este plan es muy necesario dentro de una institución, debido a que toda organización, sin importar de que tipo sea, se encuentran sometidas a cambios en todos los

niveles. Especialmente cuando se habla de cambios, las tecnologías de información son las que más sufren de este fenómeno, por lo cual es necesario tener un plan de mantenimiento que permita a la institución adaptarse a los cambios y no perder la competitividad en el modelo de negocio.

Por lo cual es necesario que todo el Plan de Contingencia se mantenga actualizado continuamente. Cuando se desee hacer cambios en el plan de contingencia, la siguiente guía será de mucha ayuda, ya que se establecen varios parámetros y mediadas que se deben considerar para la gestión de controles de seguridad de la información.

Y para ello se debe seguir un procedimiento formal, el cual se detalla en el control de Gestión de Cambios en el dominio de Seguridad en la Operativa. Este plan esta completamente basado en los dominios expuestos en la Norma ISO/IEC 27002:2013.

IMPLEMENTACIÓN Y PRUEBAS

Sistema de monitoreo NAGIOS

La implementación de un sistema de monitoreo cubre la necesidad de mejor el dominio de seguridad en las telecomunicaciones según lo que se detalla en la norma ISO/IEC 27002:2013. En este dominio se encuentra el control de red el cual dice o recomienda que es necesario administrar y controlar las redes para que información de los sistemas y aplicaciones se encuentre protegida.

NAGIOS se ha convertido en una herramienta potencial en aspecto de monitoreo en código abierto, su ambiente ofrece una vigilancia más comprensiva, para el mantenimiento y control de equipos, redes, servidores y se lo está empleando tanto en data centers como en laboratorios. Los tiempos, los equipos, los servicios que van a ser monitoreados se los configura dentro de los archivos que forman parte de esta aplicación, los mismos que se van a detallar más adelante.

NAGIOS permite gestionar hosts y servicios de forma remota en una sola ventana. Indica advertencias en los estados de los hosts o servicios y permite establecer alarmas que indica si algo va mal en sus servidores, y finalmente ayuda a los administradores de red detectar problemas antes de que ocurran. En consecuencia, ayuda a reducir el tiempo de indisponibilidad de los servicios y disminuye pérdidas empresariales.

En la Figura 12 se puede observar la interfaz web de NAGIOS con sus configuraciones correctamente aplicadas, donde los servidores de la COAC Chuchuqui Ltda. se encuentran bajo monitoreo.

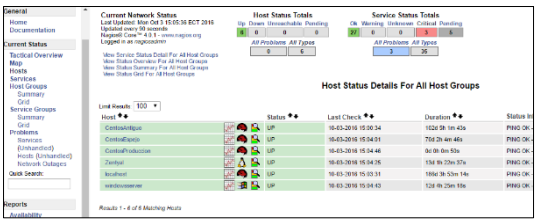

Figura 12: Servidores de la COAC Chuchuqui bajo monitoreo de NAGIOS.

Fuente: Elaboración propia.

En la Figura 13 se observa el resultado de la configuración de las gráficas con pnp4 en NAGIOS. Estas gráficas nos indican el estado de los servicios en distintos rangos de tiempo (últimas 4 horas, últimas 25 horas, última semana, último mes y último año), según se desee.

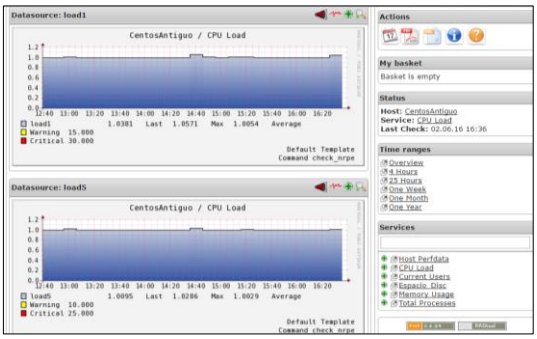

Figura 13: Gráfica pnp4 en NAGIOS del servicio de CPU Load para el servidor Centos Antiguo

Fuente: Elaboración propia.

Con la aplicación de My basket de pnp4 se puede seleccionar diferentes servicios incluso de diferentes servidores en caso de querer sacar reportes, como se muestra en la Figura 14.

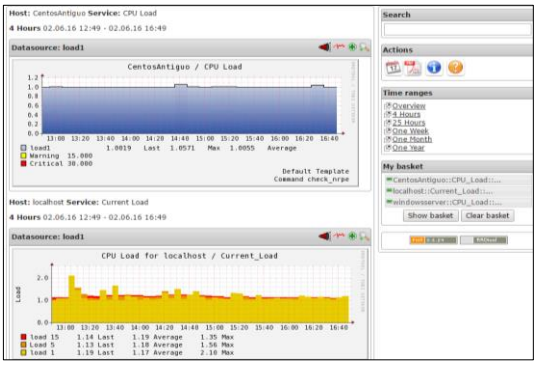

Figura 14: Selección de varios servicios con la aplicación My basket de pnp4 en NAGIOS

Fuente: Elaboración propia.

El sistema de monitoreo de Nagios se encuentra configurado de tal modo que las notificaciones de eventualidades se envían mediante mensajes de correo electrónico a los administradores de la red de la COAC Chuchuqui Ltda., como se puede observar en la Figura 15 un ejemplo.

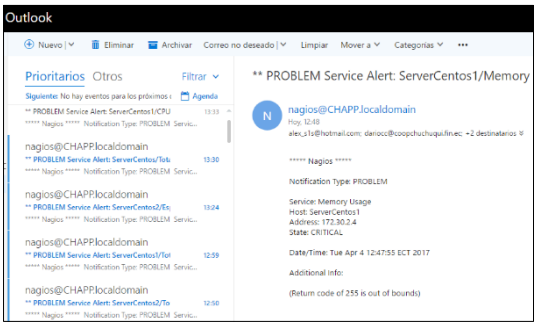

Figura 15: Notificaciones de Nagios mediante mensajes de correo electrónico

Fuente: Elaboración propia.

Control de puertos abiertos

Esta implementación mejora el dominio de control de accesos de la norma ISO /IEC 27002:2013, asegurando que ningún puerto que permita la conexión remota se encuentre habilitado o de ser el caso, mejorar la seguridad para los puertos habilitados.

Para el control de puertos se realizó un escaneó empleando el sistema operativo de Kali Linux y su herramienta de NMAP (Network Mapper) que es un escaneador de seguridad que permite descubrir host y servicios en la red. El procedimiento para este proceso es sencillo una vez que se cuente con este sistema operativo de Kali Linux, para su ejecución solo se necesita abrir un terminal e introducir el comando con la siguiente estructura:

- **[root@kali]#** nmap -sT networkAddress/netmask

Figura 16: Comando para escaneo de puertos abiertos en la red mediante nmap en Kali Linux

Fuente: Elaboración propia

CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD

La capacitación fue destinada a todo el personal de la COAC Chuchuqui Ltda., con la finalidad de lograr una concienciación y educación en los aspectos de la seguridad de la información, explicando una introducción sobre la importancia de los controles de seguridad y dar conocimiento de las nuevas políticas instauradas por el departamento de Tecnología.

La capacitación se la realizó el día jueves 15 de septiembre de 2016 en el salón de capacitaciones CHUCHUQUI Ltda., con el tema "SEGURIDAD DE LA INFORMACIÓN", con una duración de 4 horas. Los puntos a tratarse en la capacitación fueron los siguientes:

- Introducción a la seguridad de la información.
- Formas de ataques informáticos y casos de fraude en el Ecuador.
- Usuarios y contraseñas de los sistemas.
- Controles de conexión a la red.
- Políticas de uso del repositorio centralizado.
- Políticas de control de dispositivos móviles.
- Política de copias de seguridad.
- Política de control de acceso a la red y a la información.
- Clasificación de la información.
- Etiquetado y manipulación de la información.
- Manual de gestión de activos.
- Manual de seguridad física y entorno.
- Formas de protegerse ante ataques informáticos.
- Formas adecuadas de navegación.

Figura 17: Presentación ante el personal de la COAC Chuchuqui Ltda., para dar inicio a la capacitación.

Fuente: Elaboración propia

V. CONCLUSIONES

- Se implementó y aprobó un plan de contingencia por el Consejo Directivo de la cooperativa de ahorro y crédito de indígenas Chuchuqui Ltda., basándose en la norma ISO/IEC 27002 logrando mejorar los aspectos de confidencialidad, integridad y disponibilidad de la red mediante la implementación de controles de seguridad.

- Se analizó la información sobre la norma ISO/IEC 27002 referente a controles de seguridad, de la cual se alineó dichos controles a las necesidades de la COAC Chuchuqui Ltda., descartando varios de ellos debido a que no se relacionaban a las actividades que se realizan en esta institución.

- Se realizó un análisis de la situación actual mediante el levantamiento de información sobre los controles de seguridad implementados en la COAC Chuchuqui Ltda. y clasificándolos como fortalezas, oportunidades, debilidades y amenazas, lo que permitió dar partida al desarrollo del Plan de Contingencia.

- Se dio respuesta a varios de los problemas encontrados en el análisis de la situación actual, mediante el desarrollo de un análisis de riesgos, un plan de emergencia, un plan de restauración, un plan de recuperación, pruebas de verificación y un plan de mantenimiento, mejorando e implementando medidas de protección a nivel de Software y Hardware.

- La realización de pruebas de evaluación se las realizó bajo la supervisión de los miembros del Departamento de Tecnología de la COAC Chuchuqui Ltda., las cuales se cumplieron con los requerimientos necesarios obteniendo resultados positivos, lo que demostró que la implementación del plan de contingencia se realizó de forma adecuada.

- Se determinó que el proyecto si es viable según los resultados del análisis de factibilidad económica, el ROI indica que hay un buen desempeño técnico-económico, la rentabilidad económica se muestra con el cálculo del VAN, la relación costo beneficio nos indica que por cada dólar invertido se recupera USD 1,37, llegando a la conclusión de que existe un ahorro para la cooperativa a partir de los 3 años 4 meses y 26 días.

- El realizar el trabajo de grado en la COAC Chuchuqui Ltda., ha sido una experiencia satisfactoria que permitió demostrar los conocimientos adquiridos en clase logrando impartir confianza con los miembros de la institución, además de permitir tener una perspectiva más clara sobre las responsabilidades profesionales que en las instituciones financieras se imponen.

VI. BIBLIOGRAFÍA

Alegre Ramos, M., & García Hurtado, A. (2011). Razones para la seguridad de la información. En Seguridad informática Ed.11 Paraninfo (págs. 2-11). Madrid: Paraninfo.

ANSI/TIA. (2012). Telecommunications Pathways and Spaces. Arlington.

Castillo, I. G., & Medina, I. M. (2014). Manual de Practiacas ara la asignatura de seguridad informática. México.

COAC Chuchuqui Ltda. (Septiembre de 2016). COAC Chuchuqui. Obtenido de http://www.coopchuchuqui.fin.ec/

Cruz, L. C. (Septiembre de 2012). Documento de estado del arte. Obtenido de http://1984.lsi.us.es/pfe/trac/pfe-pandora/raw-attachment/wiki/WikiStart/3-Doc.Estado%20del%20Arte.pdf

Giraldo Martínez, I. K., De la Torre Morales, M. E., & Villalta Gómez, C. A. (2012). Dignóstico para la Implantación de COBIT en una Empresa de Producción. Guayaquil.

Guzmán, C. G. (2004). Introducción a la Ingeniería Económica. Bogotá: Faculta de Ingeniería.

Instituto Veracruzano de acceso a la información. (2012). Plan de contingencia informático. Veracruz.

ISO. (Octubre de 2013). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27002_5.html

ISO/IEC 27002. (2013). Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información. Geneva: ISO copyright office.

IT Governance Institute. (2007). COBIT (Control Objetives for Information and related Technology). Rolling Meadows: Algonquin Road.

John D, F. &. (2000). Fundamentos de Administración Financiera. Pearson Eduaction.

Lazzari, L. L. (2006). Control de gestión: una posibleaplicación del análisis foda. Buenos Aires: Red Cuaderno CIBAGE.

NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Aseuc.

Office of Government Commerce . (2010). Operación del servicio. Londres: TSO.

Office of Government Commerce. (2010). Operación del servicio. Londres: TSO.

Orlich, J. M. (2013). Universidad para la Cooperación Internacional. Obtenido de http://www.uci.ac.cr/descargas/AE/FODA(SWOT).pdf

Ríos, S. (2014). B-able. Obtenido de http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Tejada, E. C. (2015). Auditoría de seguridad informática. IFCT0109. Málaga: IC Editorial.

VII. BIOGRAFÍA

Dony A. Reina López, Nació en Tulcán-Ecuador el 10 de diciembre de 1992. Obtuvo el título de bachiller en Físico Matemático en la unidad educativa Hermano Miguel “La Salle” de la ciudad de Tulcán, Actualmente egresado de la carrera de ingeniería en electrónica y redes de comunicación de la Universidad Técnica del Norte.

Jaime R. MICHILENA CALDERON. Nació en Atuntaqui – Ecuador el 19 de febrero del año 1983. Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional en el año 2007. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, Obtiene su Maestría en Redes de Comunicación en la Pontificia Universidad Católica del Ecuador en el año 2016 Quito- Ecuador.

Contingency Plan for the Chuchuqui Indigenous Savings and Credit Cooperative, based on ISO/IEC 27002

Authors – Dony Anderson REINA LÓPEZ, Ing Jaime Roberto MICHILENA CALDERÓN, MSc.
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte, Avenida 17 de Julio 5-21 y José María Córdova, Ibarra, Imbabura
jlortiza@utn.edu.ec, jrmichilena@utn.edu.ec

Abstract— This project is a Contingency Plan that has its application in the COUCH Chuchuqui Ltda. Of the city of Otavalo. For its development, the international standards described by the technical union of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), as well as publications of ITIL (Information Technology Infrastructure Library), were reviewed to take A standardized model of good practice that is related to information security.

This work included a risk analysis, an emergency plan, a restoration plan, a recovery plan, tests and evaluation and a maintenance plan, which allowed to establish parameters on which it was necessary to implement safety controls.

Also within the implementation of security controls a monitoring system was set up for the COAC data center servers in a free software platform (NAGIOS), a scan of open ports in the network was carried out and precautions were taken. Must take for these, the physical security of the equipment was improved by the implementation of a fingerprint reader to control access to the Data Center as well as a security door and an air conditioning system.

A training of the cooperative's personnel on information security was carried out, which helped to improve the principles of security (reliability, integrity and availability), also revealed the new security policies established in the last quarter of the year 2016 and a guide on how to perform the classification of information.

I. INTRODUCTION

The CHUCHUQUI Savings and Credit Cooperative as a financial institution has a commitment to society to provide its partners with quality financial products and services, generating sustained growth and profitability. One of the requirements to comply with this commitment is to keep the information network safe, generating strategies that help to correct the findings identified in the audit carried out by the SEPS as expressed in circular letter SEPS-IFPS-2014-03570 February 26, 2014.

Due to the demands of the SEPS after reviewing the audit reports as manifested in the Regulation of the Organic Law of the Popular and Solidarity Economy in Art. 154 and given the importance of the information handled daily by the cooperative, Implementation of network security mechanisms that protect the data that is transmitted and interact in the data network. Deploying protection resources so that the barriers to access to the Data Center and the information that is handled or stored in them, that can generate losses to the cooperative.

It is necessary that the entity tries to achieve that the SEPS certifies that the cooperative counts on a continuity of business regarding the information technology and the realization of a contingency plan supports that the cooperative is in a stage of technological growth. In addition to providing quality services to ensure a higher level of reliability in its partners and customers.

When you have a data transfer with high levels of computer security, it allows the beneficiary to reduce operational costs, improve its viability, scalability and cost-benefit of the network structure, obtaining a great advantage to excel in the competitiveness with other entities of the same character.

II. REGULATORY AGENCIES

TECHNICAL STANDARD ISO/IEC 27002

The standard establishes guidelines and general principles to initiate, implement, maintain and improve an information security management in an organization. The objectives defined in this standard provide general guidelines on the goals generated for an information security management.

The objectives of the controls of this standard are intended to be put in place to assist the requirements generated through the analysis and evaluation of risks. This standard can serve as a practical guide to deploying the institution's information security procedures and efficient security management practices, and to generate a growing confidence in the activities that involve customers.

This standard has 14 domains of information security that together total 35 main categories and 114 security controls, in addition to an introduction of analysis and evaluation for the treatment of risks.

Domains.

Each domain has a number of major categories of information security. The 14 domains are (the numbers in parentheses represent the number of categories for each domain which are detailed in the Maintenance Plan):

• Information security policy (1)

• Organizational aspects of information security (2)

• Security linked to human resources (3)

• Asset management (3)

• Access Control (4)

• Encryption (1)

• Physical and Environmental Security (2)

• Safety in operation (7)

• Security in telecommunications (2)

• Acquisition, Development and Maintenance of information systems (3)

• Relations with suppliers (2)

• Management of security incidents of information (1)

• Aspects of information security in business continuity management (2)

• Compliance (2)

Note: The order of the domains in this rule does not mean their degree of importance. Depending on the circumstances, all sections may be important. Therefore, it is desirable that each organization that uses this standard identifies what are the applicable items, what importance they give them and their applications for specific business processes. All alignments in this standard are not ranked by priorities unless otherwise noted.

TECHNICAL STANDARD NTC/ISO 27005:2005

This standard is developed thanks to the participation of ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) which themselves are the ones that form the specialized system for standardization worldwide. In addition to these there are other bodies that form committees to deal with technical issues. When the technical committee of these higher bodies issues a new International Standard to all national organizations, it must comply with 75% approval by taking a vote.

NTC-ISO 27005 provides guidelines or guidelines that support risk management in information security for an institution, covering the requirements of an information security management system (ISMS) in relation to the standard ISO 27001.

This standard serves as a support for the successful implementation of the general controls described in ISO / IEC 27001 and ISO / IEC 27002 for information security, with its focus on risk management, so it is necessary to have prior knowledge Of these two standards. This standard applies to any organization that has in good risk analysis to meet the needs of computer security.

ITIL V3

ITIL (Information Technology Infraestructure Library) is an excerpt from publications, or books per se, that systematically describe a set of "good practices" for the management of IT services.

In view of the fact that institutions increasingly rely on information technologies for the development of their daily activities, as well as for their control and management through information systems, and that all this in turn is within a Network that may be controlled by other computer systems. Therefore, seeing all this complexity that is contained in networks and computer systems, it leads several institutions to resort to the need to have a management model for everything that makes up the IT infrastructure, which is efficient and Easy implementation.

Thus, as in the 1980s ITIL was born through the Central Computer and Telecommunication Agency of the British Government (CCTA), which thought and implemented a guide for British public sector offices to be More efficient in their work and thus reduce the costs derived from IT resources. ITIL currently belongs to the Office of Government Commerce (OGC), but can be used for its application freely.

ITIL discovered the need to carry out a study that contains a grouping of books according to structured sets in the processes that were most related, framing the large number of publications existing in eight volumes, denominated since then as ITIL v2.

Its latest version was published in 2007, branded as ITIL v3. In this version has been made a renewal of the information already published, which groups the main elements of ITIL in 5 volumes, which can currently be found with the following titles (in English original):

• ITIL v3 Service Strategy (SS)

• ITIL v3 Service Design (SD)

• ITIL v3 Service Operation (OS)

• ITIL v3 Continual Service Improvement (CST)

• ITIL v3 Service Transition (ST)

COBIT

COBIT (Control Objectives for information and related Technology) is a set of best practices for information management created by ISACA (Information Systems Audit and Control Association) with the support of the Institute of Information Governance Institute (IT Governance Institute), in 1992.

COBIT was created with the purpose of providing a guide that guarantees the adequate control and management of the information technologies, with the objective of reaching the objectives of the business plan of any organization. Therefore, COBIT is a supportive support for institutions that encompasses a set of tools that enable managers to meet control requirements, technical issues and business risks within all levels of the organization and stakeholders.

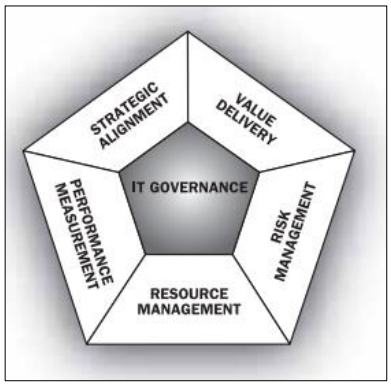

Figure 1: Areas of focus of COBIT

Source: IT Governance Institute (2007). COBIT (Control Objetives for information and related Technology). Rolling Meadows: Algonquin Road.

COBIT provides a reference frame of support that can be observed in Figure 1, which guarantees:

• IT is aligned with the business

• Enables business to maximize IT benefits

• IT resources are used responsibly

• IT risks are handled properly

III. ANALYSIS OF THE CURRENT SITUATION OF THE COOPERATIVE OF SAVINGS AND CREDIT OF INDIGENOUS CHUCHUQUI LTDA.

INFORMATION ASSETS

At present for any institution, information has become the asset with the most significant value, so there must be several methodologies for its proper storage and protection. The information of an organization can be found in different ways, can be printed documents, in digital storage units, removable disks, in databases of servers etc.

Con la finalidad de evitar pérdidas es necesario Have security controls that guarantee the principles of information (reliability, integrity and availability). The COAC does not have all the necessary controls that certify that the information is secure, for example, Figure 2 shows the lack of cabinets for the intermediate connection equipment. An analysis of the controls has been carried out, based on the technical standard ISO / IEC 27002, which is detailed in the SWOT analysis point.

Figure 2: Intermediate connection equipment without protection.

Source: Department of Technology of the COAC Chuchuqui Ltda.

With the help of the SWOT analysis you can try to cover the negative aspects of information security, knowing how to take advantage of existing controls, for example, the removable disks, hard disks and COAC backups are protected in the vault of the Institution, as this is the safest place.

DATA NETWORK

The COAC Chuchuqui has an internal network of data cabling to the different departments that comprise it, and a wireless only for devices authorized by the Department of Technology, the link is 6 Mbps. Table 1 is a description of the networks Communication.

Table 1. Communication networks of the COAC Chuchuqui.

NETWORK	DESCRIPTION
Local Network	It is made up of the cable network category 5e.
Wireless Network	It is made up of the wireless network distributed exclusively for the 2nd floor and 3rd floor.

Source: Department of Technology of the COAC Chuchuqui Ltda.

The network topology is not adequately established, it is even difficult to deduce the type of topology that is being used, because there is no labeling, the distribution to the different plants of the institution is not adequate since it does not have a distribution switch for Each floor as shown in Figure 3 COAC network topology Chuchuqui Ltda. The internet service provider is CNT EP, which supplies with single-mode 6-wire optical fiber.

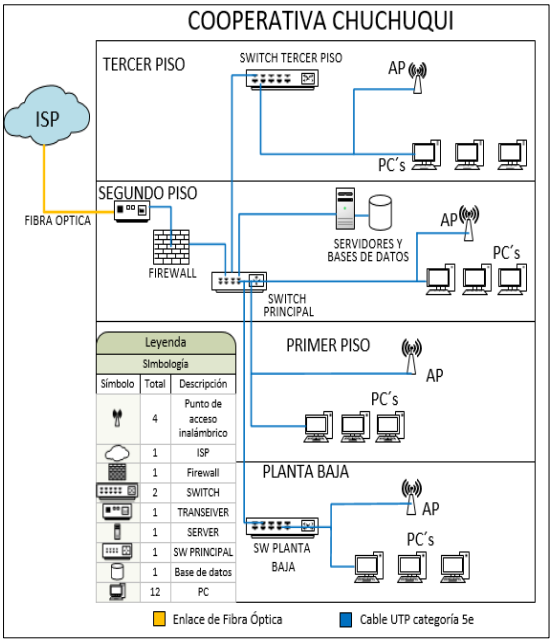

Figure 3: Network topology of the COAC Chuchuqui Ltda.

Source: Department of Technology of the COAC Chuchuqui Ltda.

The network structure and the structured cabling have been several years without being modified or renewed, so there is a need to establish a new network topology that guarantees the security of the information, considering the different rules of structured cabling.

The ANSI / EIA / TIA 569 C standard talks about the spacing for the handling of equipment and is a characteristic that has not been taken into account in the distribution of the equipment in the COUCH Chuchuqui Ltda., This standard specifies to us that Provide a rear clearance of 2 feet for service access on the back of racks and cabinets, but it is most advisable to have a back space of 1 m (3 feet) for better device handling.

Another standard that does not comply with the Chuchuqui COAC is the ANSI / EIA / TIA 568 C.1-1 which specifies how to design a telecommunications cabling system for commercial buildings, in addition to the spaces that must be handled in work areas It also shows how to plan, distribute spaces and install transmission media.

DATA CENTER

The data center area is located on the 2nd floor of the COAC and is 9m2. It consists of a floor cabinet housing the networking equipment, 4 tower servers, 1 rack server and a Panasonic analogue switchboard, also contains a 6KVA unmanaged UPS, 1 PC server outside the cabinet and a system Of electrical protection.

The Data Center lacks an air conditioning system, so the room temperatures are high, it also lacks a security door and a biometric for access only to authorized persons, as can be seen in Figure 4. In this room There is also a window, which is not recommended for a Data Center, Figure 5 shows the window seen from inside the Data Center.

Figure 4: Data Center Access Gate

Source: Department of Technology of the COAC Chuchuqui Ltda.

Figure 5: Window inside the Data Center of the COAC Chuchuqui Ltda.

Source: Department of Technology of the COAC Chuchuqui Ltda.

In addition, the Data Center must improve in aspects of the electric power supply as shown in Figure 6, also in the paint used in the walls and increase information signs of industrial safety.

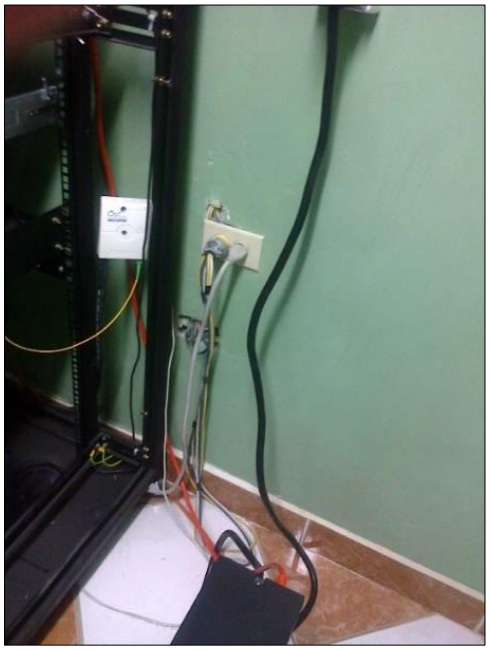

Figure 6: Power supply for equipment in the Data Center of the COAC Chuchuqui Ltda.

Source: Department of Technology of the COAC Chuchuqui Ltda.

IV. CONTINGENCY PLAN DEVELOPMENT

STRUCTURE

In Figure 7, it is possible to observe the stages in which the Contingency Plan is divided.

Figure 7: Stages of the Contingency Plan

Source: Elaboración propia.

- Risk analysis

Before an eventuality happens, any institution should try to mitigate the impacts through a risk analysis, this procedure is essential to begin to develop a Contingency Plan and have an idea of how to deal with an incident.

At this point the risks of an impact will be analyzed and depending on these will be given a priority level and it will be established which type of sub-plan is the most appropriate to start it.

Table 2 shows a description of the four sub-plans contained in the Contingency Plan, which will be operated depending on the type of contingency and risk estimation.

- Verification and evaluation tests:

Before a Contingency Plan is approved by a board of directors, it must be submitted to a series of tests, to verify that the procedures proposed in said plan, obtain the expected results, for this the personnel must be trained in the different scenarios test. At the end, an analysis of the results will be carried out and it will be determined if the Plan is appropriate for the institution.

Table 2: Contingency sub-plans

	EMERGENCY	**RESTORATION**	**RECOVERY**	**MAINTENANCE**
OBJECTIVE	Limit damage	Continue processes	Full recovery of processes	Prevent damage
PERFORMANCE	Immediately	Immediately	Short term	Continually
CONTENT	Evacuation and damage assessment	Alternatives for Significant Processes	Strategies for the recovery of all resources	Regulations, standards, security policies
MAIN RESPONSIBILITY	Users and employees of the cooperative	Department of Technology and WEBCOOP	Department of Technology	Users and employees of the cooperative

Source: Department of Technology of the COAC Chuchuqui Ltda.

RISK ANALYSIS

Identification of risk.

The main purpose of risk identification is for any organization to be able to anticipate what causes a potential loss and to understand how, where and why this loss might occur. The steps to be developed below should help to collect input data for the risk estimation activity. Figure 8 shows the percentages of different types of risks to which information systems are exposed.

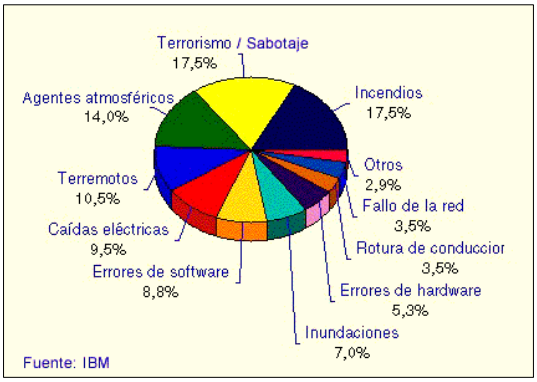

Figure 8: Risk to which the Information Systems are immersed

Source: Sánchez A. (2012). Resguardar Información: Clasificación de respaldos de la información. Recuperado el 24 de noviembre de 2016 de: http://azaleasanchez-resguardarinformacion.blogspot.com/2012/02/clasificacion-de-respaldos-de-la.html

Identification of impact.

An impact can be considered as loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc. This process allows to establish the damages or consequences that an organization suffers and that are caused by what this standard calls it as an incident scenario. An incident scenario is generated from the details of a threat, which can take advantage of a particular vulnerability or in some cases, a set of vulnerabilities of an eventuality in information security (ISO / IEC 27002, 2013).

In order to establish the impact of the incident scenarios, the impact criteria that must be defined in the context determination or, in other words, the causes of these scenarios must be identified. It is necessary to identify assets or systems are affected in each scenario. In this way, to be able to determine the value of those assets and the financial costs to which the institution is subjected.

Risk estimation.

Risk analysis can be performed with varying degrees of detail depending on the criticality of the assets, the extent of known vulnerabilities, and previous incidents involving the organization. An estimation methodology can be qualitative or quantitative, or a combination of them, depending on the circumstances. In practice, qualitative estimation is often used primarily to obtain a general indication of the level of risk and to reveal the most important risks.

The evaluation and management of these risks will allow the Cooperative to:

• Develop strategies for recovery and support of operational, technological and human decisions.

• Identify existing controls and new controls to be implemented to minimize risks by evaluating the cost / benefit of such controls.

• Plan information security.

For a correct estimation of the risks it is necessary to identify the most important processes, the main services to be reestablished, and the information that must be backed up within the institution, and depending on this importance determine the estimate or criticality of the risk.

Main Processes Identified

Software

• WEBCOOP "Corporate Web System"

• SADFIN "System of financial administration and accounting"

• ZENTYAL "Mail manager, active directory, internet, webserver, firewall, file server, etc."

Main services to be restored and / or recovered

• Windows (PC CLIENT)

-Internet.

- Microsoft Office tools.

• Base Software (SERVER)

- MySQL Server Base

• Information Backup (SERVER)

- Backup of CENTOS 5 configuration

- Backup of the WEBCOOP Database (SQL)

- Backup of the WEBSITE

- SADFIN Server Backup.

Table 3 lists the types of impacts that can cause the risks with their description and assigned valuation. This is necessary to know what priority is given to risk when proposing a solution.

Table 3. Types of Impacts of Risks

Impact	Value	Description
Critical	4	Loss of confidential information and when significant damage occurs in equipment.
High	3	When operations and functions, information of users and institutional information systems are affected
Medium	2	When the damages are partial (only occur in certain systems without affecting operations)
Low	1	When they do not affect the main activities or systems

Source: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Thus, as the types of impacts it is important to describe the types of frequency at which hazards can occur. Table 4 shows the type of frequency of occurrence of a threat.

Table 4. Types of Frequency of occurrence of a threat.

Frequency	Value	Description
Critical	5	When a risk or threat occurs from one to three times a day
High	4	When a risk or threat occurs one to three times a week
Medium	3	When a risk or threat occurs from one to three times a month
Low	2	When a risk or threat occurs one to three times a year
Unlikely	1	Its value is low as it is almost unlikely to happen or may occur once every three years or more.

Source: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Once the types of impacts and frequency types have been established, we can establish the risk estimation using the MAGERIT methodology, which compares the Impact and Frequency values, as indicated in Table 5.

Table 5. Estimation of risk according to MAGERIT analysis.

RISK		FREQUENCY				
		Critical	High	Medium	Low	Unlikely
IMPACT	Critical					
	High					
	Medium					
	Low					

Source: Own elaboration.

SWOT Analysis

This analysis has been seen as an evolution within the management and planning systems and has been part of the most important aspects of companies for survival and adaptation to new changes.

From this analysis are derived two aspects: external and internal which are grouped under the following concepts:

- External aspects. Their analysis is based on the relationship they have with the environment to which they are exposed or the current state in which they are and the changes that are expected to have in the future, taking into account that, These aspects are not controllable. Within these aspects are the concepts of opportunities and threats.
- Internal aspects. Their analysis is made based on the current state in which these are and the variables in analysis that these need to maintain the competitiveness of the whole institution in general. Since according to experts the internal aspects are those that establish the sustainability of the competitiveness. Within these aspects are the concepts of strengths and weaknesses.

Next, a summary of the objectives and controls of the ISO / IEC 27002 standard on which this SWOT analysis is based is shown in Figure 9. For this summary, some security controls were eliminated, which are not applied to CHUCUQUI COAC, since they are not related to the activities that are carried out in it.

For this analysis, the ISO / IEC 27002: 2013 standard has been taken into account, which has analyzed each of the objectives and controls in relation to the current situation of the COAC (Cooperativa de Ahorro y Crédito) And classifying each one with respect to the concepts of this methodology. Table 6 shows each description that is accompanied by the literal of the norm to which it is related.

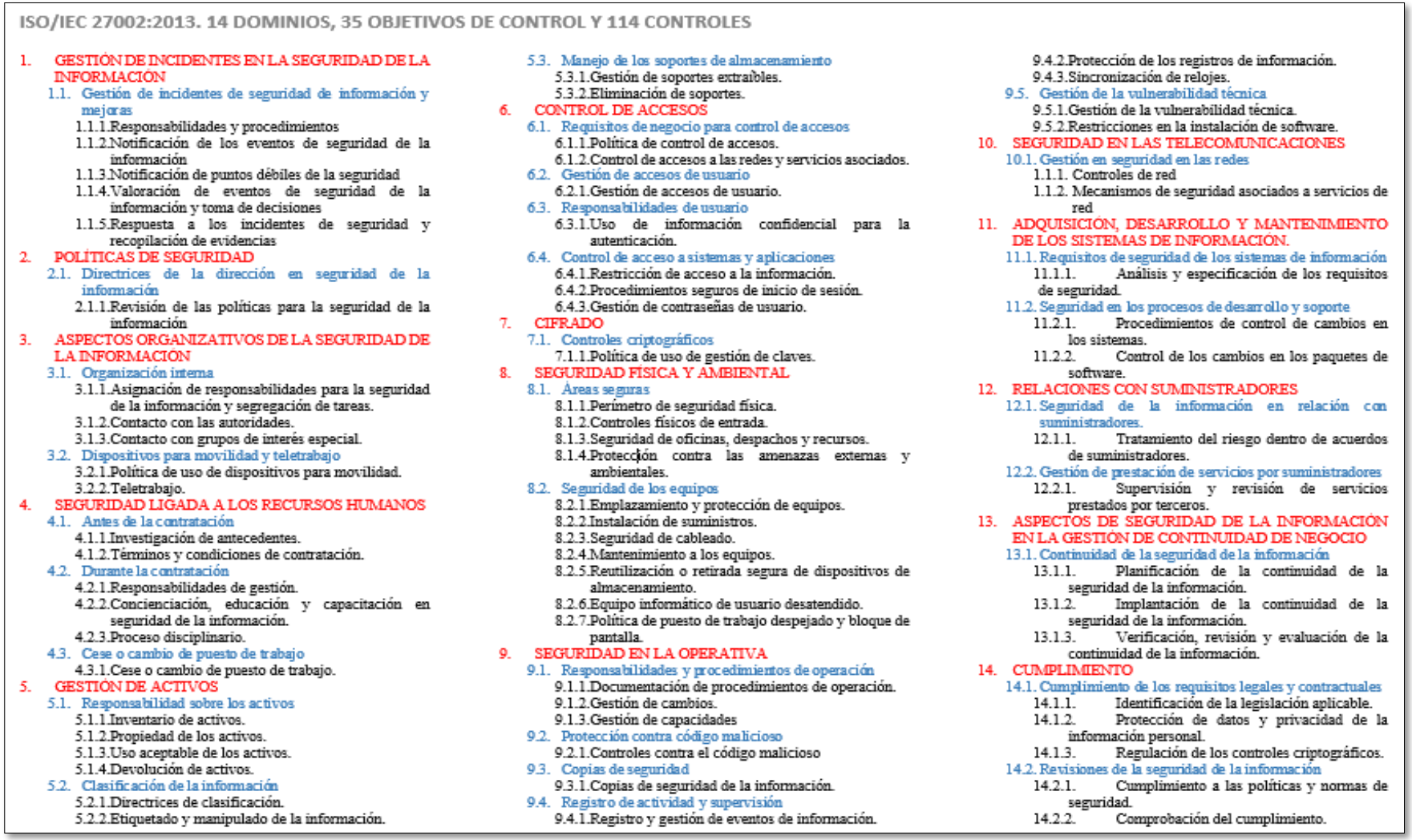

Figure 9: Standard summary ISO/IEC 27002:2013

Source: Coupling of ISO/IEC 27002:2013

Table 6. SWOT Analysis Result

S (Strengths)	O (Opportunities)	W (Weaknesses)	A (Threats)
Mobility policies and telework not established. (3.2) Contracts establish confidentiality points and responsibilities. (4.1.2) It has access control policies. (6.1) The use of good security practices in the organization is required. (6.3) Control access to systems and applications. (6.4) Key management. (7) Areas of public access are well defined. (8.1) Active computers such as servers and databases are protected and isolated from unauthorized persons. (8.2.1) There are information procedures made available to users. (9.1.1) It is a question of executing a minimum of possible changes in the security of the information, that can have some affectation in the information. The changes that are made are under supervision. (9.1.2) The servers are under monitoring and the network resources are correctly distributed through access rules. (9.1.3) All networked Laptops have licensed antivirus. (9.2) Backups of information or backups of databases are made. (9.3) The activity log of the system administrator and operator is checked. (9.4.1) All systems are synchronized. (9.4.3) There is a restriction on software installation. (9.6.2) Security measures are in place in telecommunications. (10) A technical review of the applications is made periodically after making changes to the operating systems. (11.2.1) There is a restriction on changes to software packages. (11.2.2)	Gradual creation of security policies. (1.1) There are information classification guidelines, but they have not been implemented. (5.2) It has fire detection systems and extinguishers for fire extinguishing. (8.1.3) It has UPS and generated by manual initiation energy. (8.2.2) Adequate adaptation of the policy of clear job and lock of screen. (8.2.7) An analysis and specification of safety requirements is being developed. (11.1.1) The use of engineering principles in systems protection applies. (11.2) Incident management in information security is being developed. (1) Knowledge of policies that establish service providers about information security. (12)	Officials in the technology department are not assigned responsibilities and procedures related to information security. (1.1.1) and (3.1.1) There is no model for the evaluation of information security and decision-making events. (1.1.4) The contacts of interest and management of information security are not yet defined. (3.1) There is no ongoing training on information security. (4.2.2) It has a registry of active network equipment, but is out of date. (5.1) There is no labeling and manipulation for information. (5.2.2) There is a lack of better Security aspects in offices specifically, there is no adequate signage in all sectors of the institution. (8.1.3) Protection against external and environmental threats is subject to the current architectural construction. (8.1.4) Officials lack the custom for the implementation of the policy of clear labor power. (8.2.7) There is no control for change management. (9.1.2) There is no IDS and IPS detection and prevention for controlling malicious code. (9.2) Audits of information systems have not been carried out regularly. (9.5) There is no management of technical vulnerabilities. (9.5.2) There is no periodic verification, review and evaluation of the continuity of the information. (13.1.3) There is no periodic verification of compliance with security policies and standards. (14.2)	SSH enabled access and the default port is handled. (11.1) Interconnection equipment outside the Data Center is accessible. (5.3) They do not have user access management system, access rights and special privileges. (6.2) Interconnection equipment is unprotected from interception, interference and possible damage. And the structured cabling needs do in several sectors. (8.2.3) It lacks a policy that allows and restricts the safe reuse or restriction of storage devices. (8.2.5) The necessary measures are not taken for the supervision and revision of services provided by third parties. (12.2.1)

Source: Own elaboration.

EMERGENCY PLAN

Estimation of scenarios.

The estimation of the incident scenarios allows us to determine the necessary instruments to be able to prioritize and guide the actions that will be carried out when any of these incidents happen. Thus, as well as correcting vulnerabilities and thus obtaining better results in the prevention and risk mitigation process. In Table 7 we can see examples of emergency risks with their respective measures and implementation time.

Table 7. Examples of emergency risks

RISK	MEASURE TO IMPLEMENT	IMPLEMENTATION TIME
Earthquake of 6.5 ° in the scale of Richter, of tectonic origin.	Carry out evacuation drills for staff working in the cooperative. Checking the operation of alarms. Check that there are no shelves or tables that are not susceptible to falls.	Medium term: from 6 to 9 months.
Fire	Evaluation of electrical installations to ensure the reduction of the probability of a short circuit.	Short term: from 3 to 6 months
Explosive devices	Training of security personnel, with the purpose of establishing protection measures in case of finding suspicious packages on the premises of the institution.	Medium term: from 6 to 9 months.

Source: Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de: http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Institutional response organization.

The institution must establish an institutional response organization or committee, which will be responsible for leading the emergency plan implementation process. The structure is then described graphically in Figure 10:

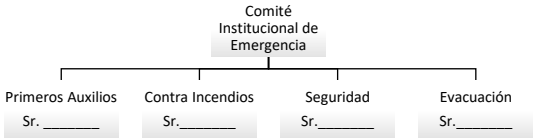

Figure 10. Institutional Emergency Committee

Source: Own elaboration.

RESTORATION PLAN

For the development of the restoration plan, it is necessary to take into account Figure 11, in which it presents a flow chart that proposes an incident management procedure structure based on ITIL.

Figure 11: Incident Management Procedure

Source: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

Restore times are based on the publication of ITIL, which also proposes a priority code system as shown in Table 8.

Table 8. Classification of restoration times

Priority code	Description	Target restoration time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours

Source: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

It should be taken into account that the impact, priority and time may vary throughout the incidence analysis as described below:

- Can be extended due to increased faults or a sequence of faults.
- Can be reduced by implementing temporary solutions that are effective in such a way that the incident is terminated.

MAINTENANCE PLAN

This plan is very necessary within an institution, because every organization, regardless of its type, is subject to change at all levels. Especially when talking about changes, information technologies are the most suffering from this phenomenon, so it is necessary to have a maintenance plan that allows the institution to

adapt to changes and not lose competitiveness in the business model.

Therefore, it is necessary that the entire Contingency Plan be continuously updated. When it is desired to make changes to the contingency plan, the following guide will be very helpful, since it establishes several parameters and mediated that must be considered for the management of information security controls.

And for this, a formal procedure must be followed, which is detailed in the control of Change Management in the Operational Security domain. This plan is completely based on the domains set forth in ISO / IEC 27002: 2013.

IMPLEMENTATION AND TESTING

NAGIOS monitoring system

The implementation of a monitoring system covers the need to improve the security domain in telecommunications according to what is detailed in ISO / IEC 27002: 2013. In this domain is the network control which says or recommends that it is necessary to manage and control the networks so that information of the systems and applications is protected.

NAGIOS has become a potential tool in open source monitoring, its environment offers more comprehensive monitoring, maintenance and control of equipment, networks and servers and is being used in both data centers and laboratories. The times, the equipment, the services that are going to be monitored are configured within the files that are part of this application, the same that will be detailed later.

NAGIOS allows you to manage hosts and services remotely in a single window. Indicates warnings in the states of the hosts or services and allows to set alarms indicating if something goes wrong on their servers, and finally helps network administrators detect problems before they occur. Consequently, it helps reduce the downtime of services and reduces business losses.

Figure 12 shows the NAGIOS web interface with its correctly applied configurations, where the servers of COAC Chuchuqui Ltda. Are under monitoring.

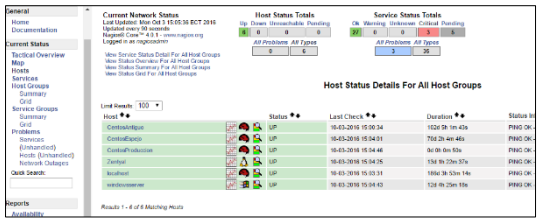

Figure 12: Chuchuqui COAC servers under NAGIOS monitoring.

Source: Own elaboration.

Figure 13 shows the result of the configuration of the graphs with pnp4 in NAGIOS. These graphs indicate the status of services in different time ranges (last 4 hours, last 25 hours, last week, last month and last year), as desired.

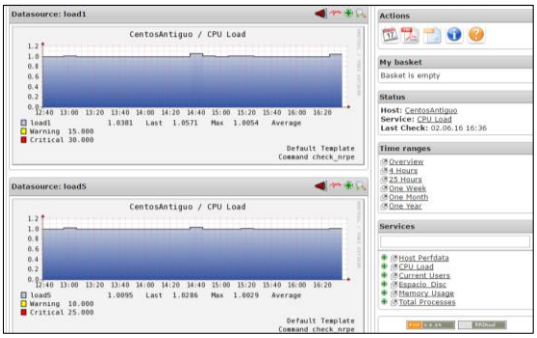

Figure 13: Graph pnp4 in NAGIOS of the CPU Load service for the old Centos server

Source: Own elaboration.

With the application of My basket pnp4 you can select different services even from different servers in case you want to take out reports, as shown in Figure 14.

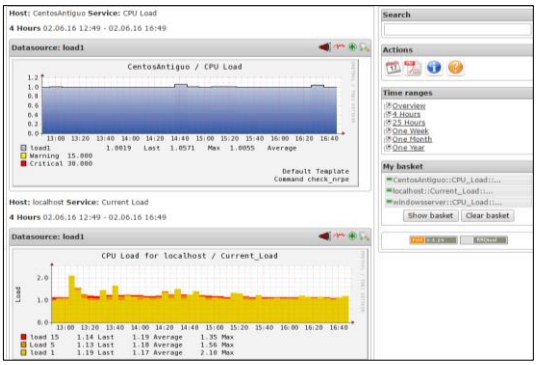

Figure 14: Selection of various services with the pnp4 My basket application in NAGIOS

Source: Own elaboration.

The monitoring system of Nagios is configured in such a way that notifications of eventualities are sent by e-mail to the administrators of the network of the COUCH Chuchuqui Ltda., As can be seen in Figure 15 an example.

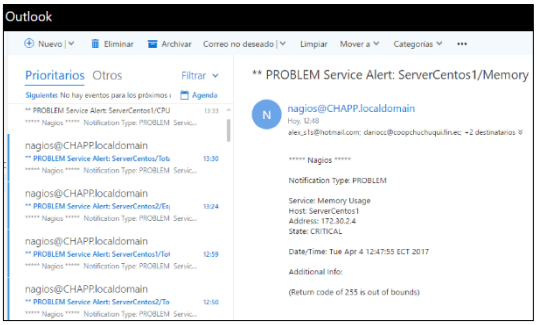

Figure 15: Nagios notifications via e-mail messages

Source: Own elaboration.

Open Port Control

This implementation improves the access control domain of ISO / IEC 27002: 2013, ensuring that no port that allows the remote connection is enabled or, if necessary, to improve the security for the enabled ports..

For port control, a scan was performed using the Kali Linux operating system and its NMAP (Network Mapper) tool, which is a security scanner that allows you to discover hosts and services on the network. The procedure for this process is simple once you have this operating system Kali Linux, for its execution only need to open a terminal and enter the command with the following structure:

• **[root@kali]#** nmap -sT networkAddress/netmask

Figure 16: Command for scanning open ports on the network using nmap on Kali Linux

Source: Own elaboration.

TRAINING IN INFORMATION SECURITY AND SECURITY POLICIES

The training was intended for all the personnel of COAC Chuchuqui Ltda., With the purpose of raising awareness and education in the aspects of information security, explaining an introduction about the importance of security controls and giving knowledge of the New policies instituted by the Department of Technology.

The training took place on Thursday, September 15, 2016 in the training room CHUCHUQUI Ltda., With the theme "SECURITY OF THE INFORMATION", with a duration of 4 hours. The points to be addressed in the training were the following:

- Introduction to information security.
- Forms of computer attacks and cases of fraud in Ecuador.
- Users and system passwords.
- Network connection controls.
- Policies for the use of the centralized repository.
- Mobile device control policies.
- Backup policy.
- Policy to control access to the network and information.
- Classification of information.
- Labeling and manipulation of information.
- Asset management manual.
- Manual of physical security and environment.
- Ways to protect against computer attacks.
- Appropriate forms of navigation.

Figure 17: Presentation to the staff of COAC Chuchuqui Ltda., To start the training.

Source: Own elaboration.

V. CONCLUSIONS

• A contingency plan was implemented and approved by the Board of Directors of the Chuchuqui Indigenous Credit Union, based on ISO / IEC 27002, improving the confidentiality, integrity and availability aspects of the network through the implementation of Security controls.

• The information on ISO / IEC 27002 regarding safety controls was analyzed, and these controls were aligned to the needs of COAC Chuchuqui Ltda., Discarding several of them because they were not related to the activities Performed in this institution.

• An analysis of the current situation was carried out by gathering information on the security controls implemented at COAC Chuchuqui Ltda. And classifying them as strengths, opportunities, weaknesses and threats, which allowed starting the development of the Contingency Plan.

• Several problems encountered in the analysis of the current situation were addressed through the development of a risk analysis, an emergency plan, a restoration plan, a recovery plan, verification tests and a maintenance plan , Improving and implementing protection measures at Software and Hardware level.

• The evaluation tests were carried out under the supervision of members of the Department of Technology of COUCH Chuchuqui Ltda., Which met the necessary requirements obtaining positive results, which demonstrated that the implementation of the contingency plan Performed properly.

• It was determined that if the project is feasible according to the results of the economic feasibility analysis, the ROI indicates that there is a good technical-economic performance, the economic profitability is shown with the NPV calculation, the cost benefit ratio tells us that for each Dollar invested recovers USD 1.37, concluding that there is a saving for the cooperative from 3 years 4 months and 26 days.

• Conducting undergraduate work at COAC Chuchuqui Ltda., Has been a satisfactory experience that allowed the demonstration of the knowledge acquired in the classroom to give confidence to the members of the institution, in addition to allowing a clearer perspective on the professional responsibilities that In financial institutions are imposed.

VI. BIBLIOGRAPHY

Alegre Ramos, M., & García Hurtado, A. (2011). Razones para la seguridad de la información. En Seguridad informática Ed.11 Paraninfo (págs. 2-11). Madrid: Paraninfo.

ANSI/TIA. (2012). Telecommunications Pathways and Spaces. Arlington.

Castillo, I. G., & Medina, I. M. (2014). Manual de Practiacas ara la asignatura de seguridad informática. México.

COAC Chuchuqui Ltda. (Septiembre de 2016). COAC Chuchuqui. Obtenido de http://www.coopchuchuqui.fin.ec/

Cruz, L. C. (Septiembre de 2012). Documento de estado del arte. Obtenido de http://1984.lsi.us.es/pfe/trac/pfe-pandora/raw-attachment/wiki/WikiStart/3-Doc.Estado%20del%20Arte.pdf

Giraldo Martínez, I. K., De la Torre Morales, M. E., & Villalta Gómez, C. A. (2012). Dignóstico para la Implantación de COBIT en una Empresa de Producción. Guayaquil.

Guzmán, C. G. (2004). Introducción a la Ingeniería Económica. Bogotá: Faculta de Ingeniería.

Instituto Veracruzano de acceso a la información. (2012). Plan de contingencia informático. Veracruz.

ISO. (Octubre de 2013). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27002_5.html

ISO/IEC 27002. (2013). Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información. Geneva: ISO copyright office.

IT Governance Institute. (2007). COBIT (Control Objetives for Information and related Technology). Rolling Meadows: Algonquin Road.

John D, F. &. (2000). Fundamentos de Administración Financiera. Pearson Eduaction.

Lazzari, L. L. (2006). Control de gestión: una posibleaplicación del análisis foda. Buenos Aires: Red Cuaderno CIBAGE.

NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Aseuc.

Office of Government Commerce . (2010). Operación del servicio. Londres: TSO.

Office of Government Commerce. (2010). Operación del servicio. Londres: TSO.

Orlich, J. M. (2013). Universidad para la Cooperación Internacional. Obtenido de http://www.uci.ac.cr/descargas/AE/FODA(SWOT).pdf

Ríos, S. (2014). B-able. Obtenido de http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

Tejada, E. C. (2015). Auditoría de seguridad informática. IFCT0109. Málaga: IC Editorial.

VII. BIOGRAPHY

Dony A. Reina López, was born in Tulcán-Ecuador on December 10, 1992. He obtained a bachelor's degree in Mathematical Physics in the educational unit Hermano Miguel "La Salle" in the city of Tulcán, currently graduated from the engineering career in Electronics and communication networks of the Universidad Técnica del Norte.

Jaime R. MICHILENA CALDERON. He was born in Atuntaqui, Ecuador, on February 19, 1983. He holds a degree in Electronics and Telecommunications at the National Polytechnic School in 2007. He is currently a lecturer in the Engineering Degree in Electronics and Communication Networks at Universidad Técnica del Norte. His Masters in Communication Networks at the Pontifical Catholic University of Ecuador in 2016 Quito- Ecuador.