ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN FINANCIERA NACIONAL BASADO EN GESTIÓN DE RIESGOS

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (MSc) EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

TANIA DEL LOURDES GUEVARA HUILCAREMA
guevarahtl@hotmail.com

DIRECTOR: ING. PAULO CRISTOBAL BERMEO MANCERO, MBA
pbermeo@cfn.fin.ec

QUITO, AGOSTO DEL 2013

DECLARACIÓN

Yo, Tania Del Lourdes Guevara Huilcarema, declaro bajo juramento que el trabajo aquí descrito es de mi propia autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

Tania Del Lourdes Guevara Huilcarema

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Tania Del Lourdes Guevara Huilcarema, bajo mi supervisión.

Ing. Paulo Bermeo M., MBA.
DIRECTOR DEL PROYECTO

DEDICATORIA

A mi amado esposo por su apoyo constante e incondicional, a mis hijos porque son mi inspiración para seguir adelante, a mis padres y hermanos, tíos y primos políticos que de una u otra forma me han apoyado para culminar este proyecto.

Tania Del Lourdes Guevara Huilcarema

AGRADECIMIENTO

A Dios, por sus infinitas bendiciones que derrama sobre mí y sobre y mi familia diariamente, que por su bondad y misericordia me ha permitido llegar a estas instancias de mis estudios.

A José, mi esposo por su apoyo constante e incondicional, paciencia e infinito amor que en cada instante me demuestra.

Al Ing. Paulo Bermeo, por su guía, colaboración y disponibilidad en el desarrollo de esta tesis.

Tania Del Lourdes Guevara Huilcarema

CONTENIDO

TABLAS

FIGURAS

RESUMEN

El objetivo primordial de este proyecto de tesis es el proponer un modelo para la gestión de Seguridad de la Información para la Corporación Financiera Nacional basado en gestión de riesgos, su enfoque es estructurar, optimizar y mejorar la gestión que realiza el Departamento Nacional de Seguridad Informática y apoyar a la continuidad del negocio.

Para el efecto, se investigó y evaluó ISO/IEC 27005:2008, MAGERIT y COSO ERM, norma, metodología y marco de trabajo internacionalmente aceptadas a fin de formular una metodología de gestión de riesgos a la medida de la CFN.

En base a la metodología de gestión de riesgos formulada, se realizó un ejercicio de análisis y evaluación de riesgos, obteniendo los principales requerimientos del negocio respecto a seguridad y el plan de seguridad de la información; sobre esta base se diseñó el modelo para la gestión de Seguridad de la Información para la CFN.

Finalmente, se validó la aplicabilidad del modelo propuesto, teniendo que se logró una primera aplicación exitosa de la metodología de gestión de riesgos de seguridad de la información, demostrando que se ajusta a la realidad organizacional y presupuestaria de la CFN; por otro lado, la evaluación del impacto del modelo de gestión de seguridad propuesto, actualmente es de un 30%, una vez que finalice su implementación se pretende llagar al 80%, complementariamente, se evidencia la aplicabilidad de la propuesta dado que se lo ha venido implementando efectivamente, este impacto logrado cumple con lo formulado en la propuesta planteada en esta investigación.

CAPITULO I. INVESTIGACIÓN Y DETERMINACIÓN DE ASPECTOS COMPLEMENTARIOS EN LAS NORMAS Y METODOLOGÍAS DE GESTIÓN DE RIESGOS

1.1. INTRODUCCIÓN

Como punto de partida para la elaboración del presente trabajo de tesis, en este capítulo se propone investigar las normas y metodologías ISO/IEC 27005:2008, MAGERIT y COSO ERM, ya que en nuestro medio, son las más conocidas y/o empleadas para procesos de gestión de riesgos; el propósito fundamental es determinar aspectos complementarios entre sí, dicho análisis permitiría establecer una metodología para gestión de riesgos especializada en seguridad de la información y enfocada a la Corporación Financiera Nacional.

La gestión de riesgos es reconocida como una parte integral de buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones. Administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas[1].

1.2. OBJETIVOS

- Establecer aspectos claves que viabilicen una investigación objetiva de las diferentes metodologías y normas de gestión de riesgos propuestas

[1] AS/NZS 4360:1999, Administración de Riesgos, página 3

- Investigar y obtener los aspectos relevantes determinados en el primer objetivo de:
    - MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
    - Norma ISO 27005:2008 –Tecnología de la Información, Técnicas de Seguridad, Gestión de Riesgos de Seguridad de la Información
    - Gestión de Riesgos Corporativos – Marco Integrado (COSO ERM)
- Analizar y determinar aspectos complementarios entre las metodologías y normas investigadas

1.3. ASPECTOS CLAVES PARA LA INVESTIGACIÓN

Con la finalidad de realizar una investigación objetiva de cada una de las metodologías, normas o marcos de referencia objeto de este estudio, es indispensable definir y enfocarse en determinados aspectos claves, que permitan compararlas y establecer cómo se pueden complementar entre sí.

Entre los principales aspectos a analizar podemos citar a los siguientes:

- Visión general - alcance
- Visión específica
- Técnicas[2] de identificación de riesgos
- Técnicas de evaluación de riesgos
- Técnicas de tratamiento de riesgos

[2] Se considera técnica al conjunto de heurísticas y procedimientos que se apoyan en estándares, es decir, que utilizan una o varias notaciones específicas en términos de sintaxis y semántica y cumplen unos criterios de calidad en cuanto a la forma de obtención del producto asociado (MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, III - Guía de Técnicas, página 4).

1.4. MAGERIT VERSIÓN 2 – METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE SISTEMAS DE INFORMACIÓN

1.4.1. VISIÓN GENERAL - ALCANCE

MAGERIT, elaborada por el Consejo Superior de Administración Electrónica CSAE del Ministerio de Administraciones Públicas - España, nace como respuesta a la creciente dependencia de las organizaciones en las tecnologías de información.

Según MAGERIT, una adecuada y oportuna gestión de riesgos permite recomendar a la Dirección las medidas de protección apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducirlos al mínimo.

MAGERIT, tiene tres objetivos principales relacionados con la concienciación a los responsables de los sistemas de información, ofrecer un método sistemático para análisis de riesgos, y, mantener los riesgos identificados bajo control.

El alcance de esta metodología se enmarca en la gestión de riesgos de las tecnologías de información, específicamente en los "sistemas de información"[3] y su entorno.

Por el contexto anterior, se puede inferir que MAGERIT se centra en la gestión de riesgos de aplicaciones informáticas, datos procesados

---

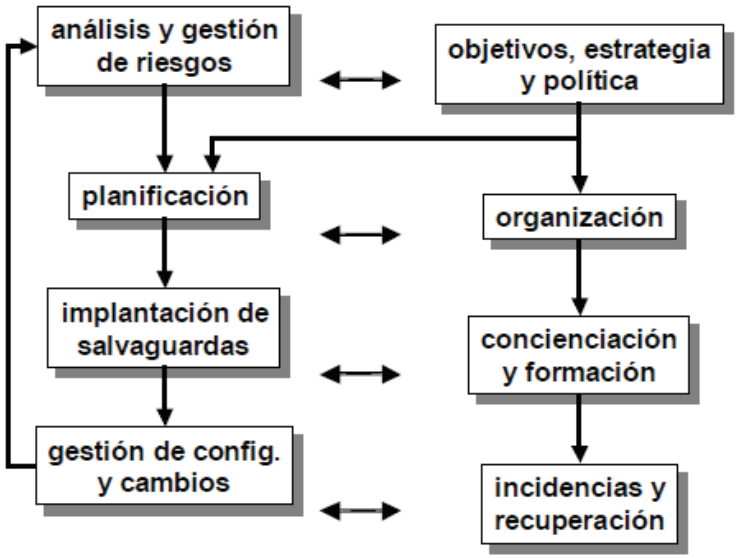
[3] Sistemas de información: los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso protección y mantenimiento (MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, I - Método, página 108).

electrónicamente, y, los componentes que los soportan (hardware, software y comunicaciones).

1.4.2. VISIÓN ESPECÍFICA

El análisis y gestión de riesgos en su contexto está planteado por MAGERIT conforme a la siguiente figura:

Figura No 1.1: Proceso de análisis y gestión de riesgos en su contexto



Fuente: *MAGERIT v2, I - Método*
Elaborado por: *Tania Guevara H.*

El análisis y gestión de riesgos debe ser una actividad periódica puesto que los sistemas de información son modificados o actualizados continuamente, y residen en un contexto cambiante (nuevos activos y nuevas amenazas).

Del análisis de riesgos se deriva un plan de seguridad que contiene los proyectos y actividades para la implantación de las salvaguardas requeridas; dicho plan debe ser alimentado considerando los objetivos, estrategias y políticas de seguridad organizacionales.

La implantación de salvaguardas debe considerar adicionalmente la concienciación al recurso humano en materia de seguridad, direccionado a la creación de una cultura de seguridad.

El personal involucrado (en cualquier punto del proceso) debe estar consciente de su papel y relevancia continua para prevenir problemas y reaccionar cuando se produzcan[4].

Para desarrollar un proyecto de análisis y gestión de riesgos, conceptualmente MAGERIT contempla tres grandes procesos:

Proceso 1: Planificación

- Estudio de oportunidad
- Determinación del alcance
- Planificación del proyecto
- Lanzamiento del Proyecto

Proceso 2: Análisis de riesgos

- Identificación, dependencia y valoración de activos
- Identificación y valoración de amenazas
- Identificación y valoración de salvaguardas existentes
- Estimación del impacto y riesgo, e, interpretación de resultados

Proceso 3: Gestión de riesgos

- Toma de decisiones
- Plan de seguridad
- Ejecución del plan

[4] MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, página 9.

Por cada uno de los procesos y/o tareas MAGERIT estable objetivos, entradas, productos de salida, técnicas a emplear y los participantes.

La identificación de riesgos se la realiza en su segundo proceso denominado Análisis de Riesgos, para cumplir los objetivos de manera ordena el proceso se basa en las denominadas "dimensiones de seguridad"[5] que de acuerdo a la metodología planteada por MAGERIT, son confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, distinguiendo sobre las dos últimas entre el uso de los servicios y el acceso a los datos.

Complementariamente, debido a la complejidad que puede tomar un proyecto de análisis y gestión de riesgos, MAGERIT recomienda el uso de herramientas automatizadas, para el efecto, PILAR – Procedimiento Informático-Lógico para el Análisis de Riesgos, es una herramienta desarrollada bajo especificaciones del Centro Nacional de Inteligencia de España y soporta íntegramente esta metodología.

1.4.3. TÉCNICAS DE IDENTIFICACIÓN DE RIESGOS

MAGERIT, proporciona el Libro III - Guía de Técnicas como medio de consulta para facilitar la ejecución del análisis y gestión de riesgos; esta guía contempla técnicas específicas y técnicas generales las mismas que no son de cumplimiento obligatorio.

De acuerdo a la metodología propuesta por MAGERIT, para llegar a identificar un riesgo, es necesario en primera instancia identificar y valorar los activos del sistema de información, sus amenazas, y las salvaguardas implementadas.

---

[5] Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor (MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, página 104).

Para la identificación, determinación de dependencias y valoración de activos, las técnicas propuestas por MAGERIT son de carácter general:

- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas
- Reuniones
- Valoración Delphi[6]

Las tareas de identificación y valoración tanto de amenazas como de salvaguardas se apoya en catálogos de amenazas y de salvaguardas respectivamente, y en las siguientes técnicas:

- Árboles de ataque
- Entrevistas
- Reuniones
- Valoración Delphi

Una vez que se han cumplido con las tareas anteriormente descritas, la identificación del riesgo se basa en las siguientes técnicas específicas:

- Análisis mediante tablas
- Análisis algorítmico

[6] "Delphi" es la forma inglesa de pronunciar Delfos, población griega famosa por su oráculo. Pese al origen fonético, el método usado por el Oráculo de Delphos (adivinación) no tenía nada que ver con el usado con el método Delphi (consenso de opinión entre expertos). Delphi basa la calidad de sus resultados en la hipótesis de que cuando no existe un conocimiento preciso de la realidad, lo mejor que se puede hacer es recoger la opinión, consensuada, de un grupo lo más amplio posible de expertos en la materia (MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Guía de Técnicas, página 68).

El análisis mediante tablas ayuda a la obtención sencilla de resultados, y, un análisis mediante técnicas algorítmicas obtiene resultados más elaborados.

MAGERIT presenta varios enfoques algorítmicos, entre los que podemos citar a: modelo cualitativo (valoración relativa del riesgo que corre un activo), modelo cuantitativo (riesgos expresados en términos de costos), modelo escalonado (análisis del impacto de la disponibilidad de los sistemas de información), y, modelo de estimación de la eficacia de las salvaguardas.

1.4.4. TÉCNICAS DE EVALUACIÓN DE RIESGOS

La evaluación de riesgos conforme la metodología MAGERIT se ejecuta en las tareas de interpretación de resultados (priorización los activos) y calificación de riesgos (por ejemplo: crítico, grave, apreciable o asumible); entre las técnicas que propone la metodología podemos citar a:

- Técnicas gráficas (gráficas: GANTT, histogramas, diagramas de Pareto y de tarta[7])
- Reuniones
- Presentaciones
- Valoración Delphi

[7] Estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360º de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica, (MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Guía de Técnicas, página 59).

1.4.5. TÉCNICAS DE TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos identificados y calificados se plasman en el Plan de Seguridad de la Información, su elaboración se apoya en las siguientes técnicas:

- Análisis Costo - Beneficio
- Planificación de proyectos

Es importante destacar que MAGERIT considera que la única forma de afrontar la complejidad propia de un proyecto de análisis y gestión de riesgos es centrarse en lo más importante, es decir, se debe comenzar a tratar los riesgos que resulten con máximo impacto y máximo riesgo.

1.5. NORMA ISO/IEC 27005:2008 – TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

1.5.1. VISIÓN GENERAL – ALCANCE

La norma ISO/IEC 27005, elaborada por el subcomité SC 27 Técnicas de Seguridad que forma parte del comité técnico ISO/IEC JTC 1 Tecnologías de Información, este comité ha sido establecido conjuntamente por ISO – Organización Internacional de Normalización e IEC – Comisión Electrónica Internacional.

El Instituto Ecuatoriano de Normalización INEN, ha editado y adoptado como ecuatoriana la Norma ISO/IEC 27005:2008, por lo que es de especial interés trabajar con la Norma Técnica Ecuatoriana NTEISO/IEC 27005.

El alcance de esta norma se enmarca en proporcionar las directrices para la gestión del riesgo enfocada a la seguridad de la información y aplicada a

una organización sea en su totalidad o una parte de ella, por ejemplo, un departamento, una ubicación física, un servicio, un sistema de información o cualquier aspecto particular de control como la planificación de la continuidad del negocio[8].

Complementariamente, la norma ISO/IEC 27005 brinda soporte particular para obtener los requisitos de un sistema de gestión de seguridad de la información (SGSI); no constituye una metodología para gestionar riesgos dejando a libertad de las organizaciones el seleccionar la metodología que mejor se ajuste a sus necesidades.

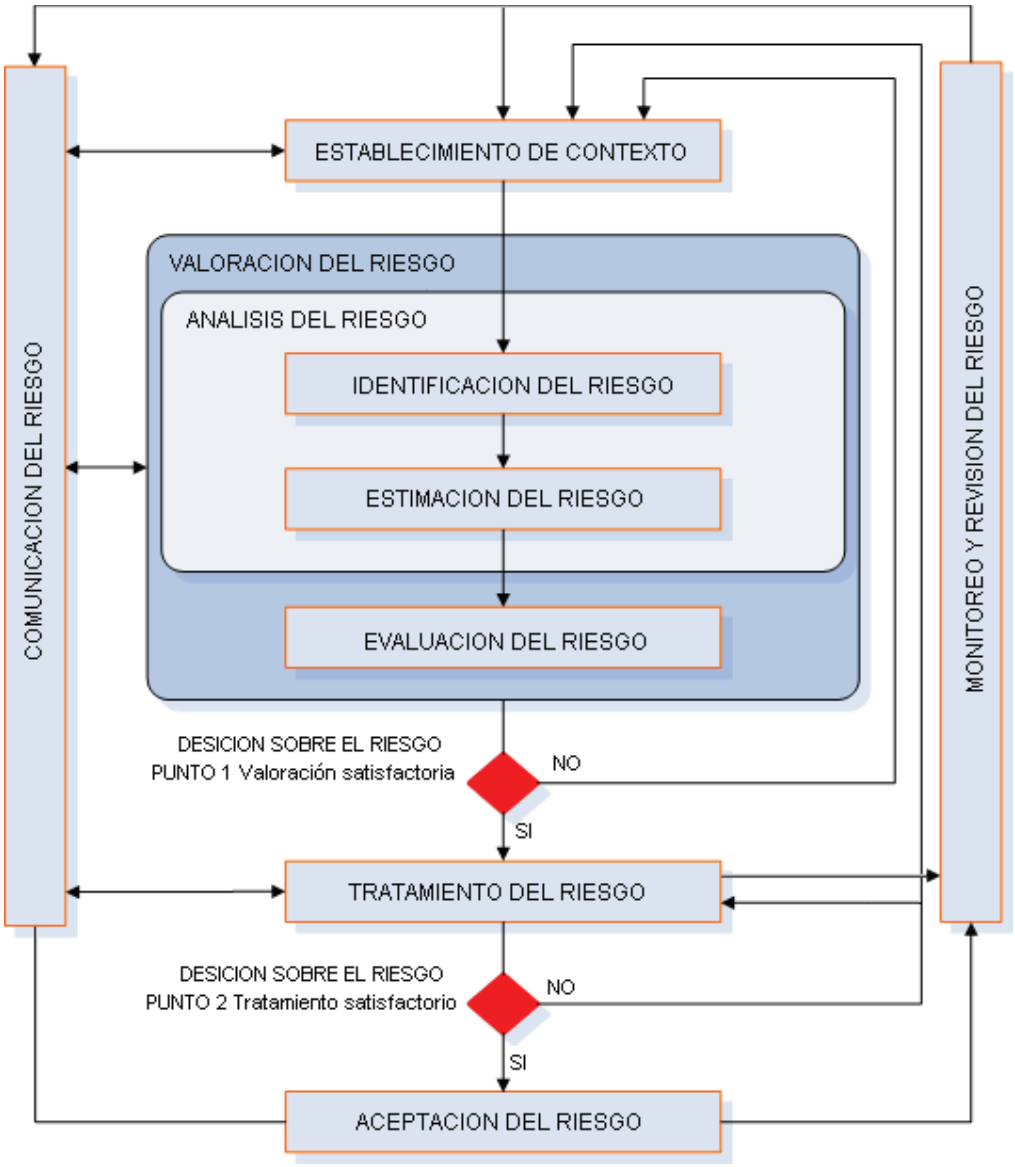
1.5.2. VISIÓN ESPECÍFICA

Para la gestión de riesgos en seguridad de la información, la norma ISO/IEC 27005, propone un esquema de procesos genérico, asegura su aplicabilidad a todo tipo de empresa u organización sin importar su tamaño (pequeña, mediana, grande), naturaleza (pública, privada, con o sin fines de lucro, entre otras) o giro de negocio (industrial, alimentos, construcción, tecnología, etc.) o tipo (proveedor, consultor, cliente, entre otros).

La siguiente figura sintetiza el proceso de gestión de riesgos de seguridad de la información:

[8] NTEISO/IEC 27005 – Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información, página 4.

Figura No 1.2: Proceso de gestión del riesgo de seguridad de la información



Fuente: *Norma Técnica NTEISO/IEC Ecuatoriana 27005*
Elaborado por: *Tania Guevara H.*

Conforme la norma ISO/IEC 27005, todo proceso de gestión de riesgos debe estar delimitado por un alcance específico, el mismo que se estable en el primer proceso de la figura 1.2 - Establecimiento del Contexto, en esta primera etapa se establecen adicionalmente, la organización para la gestión de riesgos de seguridad de la información y los criterios básicos entre los cuales se pueden destacar a criterios de evaluación del riesgos, criterios de impacto, criterios de aceptación del riesgo, entre otros.

Una vez se ha delimitada la gestión de riesgos de seguridad de la información, inmediatamente se procede a analizar y evaluar los riesgos, a este proceso la norma lo denomina Valoración del Riesgo; si la valoración de los riesgos[9] resultante satisface las necesidades de la organización y/o cumple con las especificaciones de los criterios de aceptación del riesgo establecido en el primer proceso se procede a dar tratamiento a los riesgos identificados, caso contrario, los procesos uno y dos se repiten iterativamente hasta llegar a un nivel aceptable de riesgo.

El proceso de Tratamiento del Riesgo tiene por objeto seleccionar controles para reducir, retener, evitar o transferir los riesgos y definir un plan para el tratamiento de los mismos[10]. Una vez ejecutado este paso, nuevamente es pertinente evaluar si el tratamiento que se dará a los riesgos identificados es coherente con el contexto definido para la gestión del riesgo en la seguridad de la información, en caso afirmativo se continúa con el proceso de Aceptación del Riesgo, caso contrario se deberá retomar y revisar los pasos uno, dos y tres.

Mediante el proceso de Aceptación del Riesgo, se registra de manera formal la decisión de aceptar los riesgos y las responsabilidades de dicha decisión[11]; seguido se procede con la Comunicación de los Riesgos de la seguridad de la información, a través del cual se busca intercambiar y/o compartir la información acerca de los riesgos entre quien toma la decisión y las partes involucradas con el objeto de lograr acuerdos y compromisos sobre la manera de gestionar los riesgos[12].

---

[9] Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización (NTEISO/IEC 27005 – Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información, página 11).

[10] Ídem, página 21.

[11] Ídem, página 26.

[12] Ídem, página 26.

Finalmente se debe Monitorear y Revisar el riesgo de la seguridad de la información a fin de identificar oportunamente todo cambio sea en el contexto de la organización, así como, en modificaciones de activos, amenazas, vulnerabilidades o incidentes de la seguridad de la información[13]; la ejecución de este proceso es indispensable ya que contribuye a la mejora continua.

La norma ISO/IEC 27005 describe entradas/insumos, acciones recomendadas, guías de implementación, y resultados esperados para cada uno de los procesos y/o actividades propuestas, complementariamente, facilita información adicional para las actividades de la gestión del riesgo de seguridad de la información como listados (descripción) o ejemplos de identificación y valoración de activos, valoración del impacto, amenazas comunes, vulnerabilidades y métodos para su valoración, enfoques de valoración del riesgo, restricciones para la reducción del riesgo, entre otros.

A continuación se lista los procesos y actividades que conceptualmente contempla la norma ISO/IEC 27005:

Proceso 1: Establecimiento del Contexto

- Definición de criterios básicos (evaluación del riesgo, impacto y aceptación del riesgo, etc.)
- Definición de alcance y límites
- Definición de la organización

Proceso 2: Valoración del Riesgo

- Análisis del riesgo

13 Un incidente de seguridad es un evento adverso inesperado o no deseado en un sistema de cómputo que amenaza la confidencialidad, integridad, disponibilidad y/o confiabilidad de la información, y tiene una probabilidad significativa de comprometer las operaciones del negocio (Política de Seguridad de la Información – CFN, página 2).

- Identificación del riesgo
  - Identificación de activos
  - Identificación de amenazas
  - Identificación de controles existentes
  - Identificación de vulnerabilidades
  - Identificación de consecuencias
- Estimación del riesgo
  - Valoración de las consecuencias
  - Valoración de los incidentes
  - Nivel de estimación del riesgo
- Evaluación del riesgo

Proceso 3: Tratamiento del Riesgo

- Reducción del riesgo
- Retención del riesgo
- Evitación del riesgo
- Transferencia del riesgo

Proceso 4: Aceptación del Riesgo

Proceso 5: Comunicación de los Riesgos

Proceso 6: Monitoreo y Revisión del Riesgo

- Monitoreo y revisión de los factores del riesgo
- Monitoreo, revisión y mejora de la gestión de riesgos

1.5.3. TÉCNICAS DE IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo conforme la norma ISO/IEC 27005, se lleva a cabo en el proceso de Análisis del Riesgo; la norma no facilita técnicas directamente, sin embargo, proporciona una guía de implementación de la cual se puede deducir las siguientes técnicas:

Técnicas generales:

- Reuniones
- Entrevistas
- Encuestas, entre otros.

Técnicas específicas:

- Considerar que los sistemas de información constan de más elementos que sólo hardware y software para identificar activos de información
- Designar propietarios de los activos de información con sus responsabilidades
- Obtener de los propietarios del activo, usuarios, personal de recursos humanos, administradores de las instalaciones, especialistas en seguridad de la información, expertos en seguridad física, área jurídica, experiencia interna de incidentes, entre otros, las amenazas a las que están expuestos los activos, procesos y sistemas de la organización
- Consultar y apoyarse en catálogos de amenazas, vulnerabilidades e impactos para la identificación de los mismos
- Aplicar análisis de vulnerabilidades
- Aplicar procesos de Ethical Hacking (penetración)
- Revisar los documentos que contengan información sobre controles existentes y planificados, adicionalmente verificar que los controles ya implementados funcionan adecuadamente
- Obtener de las personas responsables (de seguridad, administradores, operadores, usuarios, etc.) los controles existentes.
- Revisar resultados de auditorías para validar la eficacia de los controles existentes
- Evaluar las posibles pérdidas de confidencialidad, integridad y disponibilidad que los activos de información y procesos de negocio pueden sufrir en un escenario de incidente de seguridad a fin de identificar su impacto (consecuencias)

1.5.4. TÉCNICAS DE EVALUACIÓN DE RIESGOS

La norma ISO/IEC 27005, propone una guía de implementación del proceso de Evaluación del Riesgo, de la cual se pueden destacar las siguientes técnicas:

- Emplear metodologías sea cuantitativa (utilizando una escala de valores numéricos, apoyándose en datos históricos) o cualitativa (utilizando una escala de atributos calificativos que describa la magnitud de las consecuencias o impacto) para la estimación del riesgo.
- Para la valoración de las consecuencias:
  - Realizar un análisis de impacto del negocio (BIA)
  - Modelar los resultados de un evento o grupo de eventos
  - Extrapolar a partir de estudios experimentales o datos anteriores
- Para la valoración de los incidentes:
  - Técnicas de estimación cualitativas o cuantitativas
  - Considerar la experiencia y las estadísticas aplicables para la probabilidad de la amenaza
  - Considerar las vulnerabilidades, tanto individuales como en conjunto
- Centrarse más en el negocio y el ambiente operativo que en los elementos tecnológicos, aplicando una valoración de alto nivel para la valoración de riesgos en la seguridad de la información
- Utilizar matrices (tablas) con valores predefinidos considerando combinaciones del valor del activo, probabilidad de ocurrencia de una amenaza, facilidad de explotación de la misma, clasificación de amenazas, niveles de vulnerabilidad, entre otros, a fin de facilitar la estimación del riesgo en forma detallada

1.5.5. TÉCNICAS DE TRATAMIENTO DE RIESGOS

A fin de abordar el tratamiento de riesgos de seguridad de la información, la norma ISO/IEC 27005 propone una guía de implementación que entre otras técnicas describe a las siguientes:

- Aplicar las opciones de tratamiento del riesgo (reducción, retención, evitación, transferencia) de forma conveniente (no se excluyen mutuamente)
- Concienciación en materia de seguridad de la información
- Clasificación del riesgo
- Análisis Costo-Beneficio
- Considerar requisitos legales y reglamentarios
- Considerar el retiro de una actividad o un conjunto de actividades planificadas o existentes mediante el cambio de condiciones bajo las cuales se efectúa tal actividad
- Compartir riesgos con partes externas (contratación o subcontratación)
- Formalizar la decisión de aceptación de los riesgos finales por parte de los directores de la organización
- Desarrollar planes de comunicación continua del riesgo para las operaciones normales así como para las situaciones de emergencia

1.6. GESTIÓN DE RIESGOS CORPORATIVOS – MARCO INTEGRADO (COSO ERM)

1.6.1. VISIÓN GENERAL – ALCANCE

Gestión de Riesgos Corporativos – Marco Integrado, es un informe elaborado y propuesto por el Committee of Sponsoring Organizations of the Treadway Commission (COSO), también conocido como COSO ERM (Enterprise Risk Manager) o COSO II.

En primera instancia COSO emitió el documento “Control Interno – Marco Integrado” que ha brindado un apoyo fundamental a las organizaciones para la consecución de sus objetivos, tras su éxito y con la relevancia que ha ido tomando el concepto de gestión de riesgos, COSO percibe la necesidad de desarrollar un margo integrado para la gestión de riesgos corporativos que defina las pautas y conceptos fundamentales así como una terminología común en esta área[14].

COSO ERM, pretende profundizar la gestión del control interno de las organizaciones enfocándose en la gestión de sus riesgos, facilitando un enfoque más extenso y sólido sobre el tema de la gestión de riesgos de las empresas[15], de ninguna maneja sustituye a los procesos de gestión de control interno que cada organización debería aplicar.

Conforme el marco integrado de COSO ERM, la gestión de riesgos tiene un alcance y enfoque corporativo, de acuerdo a este marco, una entidad existe con el fin último de generar valor para sus grupos de interés, la gestión de riesgos corporativos apoya directamente a la consecución de este fin, cuando la dirección establece una estrategia y objetivos para encontrar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, además de desplegar recursos eficaz y eficientemente a fin de lograr los objetivos de la entidad[16].

1.6.2. VISIÓN ESPECÍFICA

COSO ERM, tiene como objetivo capacitar y ayudar a la dirección de una organización a identificar, evaluar y gestionar sus riesgos con la finalidad de crear y conservar su valor; está diseñado para identificar los eventos

---

[14] COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 7.

[15] Ídem, página 9.

[16] Ídem, página 15.

potenciales que puedan afectar a la entidad y gestionar los riesgos para que estén dentro del riesgos aceptado por ella, facilitando una seguridad razonable respecto al logro de sus objetivos[17].

Para COSO ERM los eventos potenciales pueden afectar a una organización en forma positiva o negativa, las posibles afectaciones positivas representan oportunidades, en tanto que las afectaciones con repercusión negativa son los riesgos; el marco integrado propone tratar ambos oportunidades y riesgos de forma tal que se apoye en el proceso de alcanzar los objetivos institucionales.

Para la gestión de riesgos corporativos, COSO ERM determina ocho componentes, cuatro categorías de objetivos organizacionales, todos relacionados entre sí y con las diferentes áreas (unidades) que conforman la entidad. La figura 1.3 representa mediante una matriz tridimensional la relación que existe entre componentes, objetivos y estructura organizacional.

[17] COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 25.

Figura No 1.3: Relación entre componentes, objetivos y estructura organizacional

Fuente: *COSO ERM, Gestión de Riesgos Corporativo – Marco Integrado*
Elaborado por: *Tania Guevara H.*

En el cubo se visualiza en forma horizontal (filas) a los ocho componentes de la gestión de riesgos corporativos, verticalmente (columnas) se encuentran las cuatro categorías de objetivos, y en la tercera dimensión del cubo las diferentes áreas o unidades de la entidad.

Componentes de la gestión de riesgos corporativos:

Ambiente interno: constituye la base de los demás componentes de la gestión de riesgos corporativos, establece la filosofía y cultura respecto a dicha gestión, se basa en la integridad y valores éticos, el riesgo aceptado[18], la supervisión ejercida por el consejo de

[18] El riesgo aceptado es el volumen de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en su búsqueda de valor, refleja su filosofía de gestión de riesgos e influye en la cultura y estilo operativo (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 31).

administración[19], la forma en que la dirección asigna la autoridad y responsabilidad y organiza a sus empleados.

Establecimiento de objetivos: mediante este componente se busca asegurar que una vez establecida la estrategia[20] y los objetivos organizacionales, cada entidad pueda evaluar sus riesgos y dar respuesta a ellos, fijando objetivos que deberán estar alineados al riesgo aceptado por la entidad y su tolerancia al riesgo, este proceso apoya directamente a la consecución de los objetivos corporativos.

Identificación de eventos: se debe identificar los acontecimientos que puedan afectar a la organización, y, determinar si corresponden a oportunidades o riesgos; para el caso de riesgos la entidad deberá evaluarlos y dar respuesta a los mismos; en caso de oportunidades, deberá considerarlos en su estrategia y proceso de establecimiento de objetivos.

Evaluación de riesgos: los eventos negativos se analizarán considerando su probabilidad de ocurrencia y el impacto que de ocurrir se producirá en la organización, para el efecto se apoya en métodos cuantitativos o cualitativos o una combinación de ambos; con el resultado de dicha evaluación, la dirección determinará la forma más adecuada para gestionarlos; conforme el marco

---

[19] El consejo de administración es un grupo colegiado (directivos, técnicos y otros con conocimiento profundo de la entidad) que asegura que la dirección mantiene una adecuada gestión de riesgos corporativos (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 41).

[20] La estrategia de una organización constituye la base para la fijación de objetivos estratégicos, operativos, de información y de cumplimiento (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 47).

integrado, los riesgos deberán ser evaluados desde una doble perspectiva: riesgo inherente[21] y riesgo residual[22].

Respuesta a los riesgos: mediante este componente se debe seleccionar las posibles respuestas a los riesgos identificados como relevantes; dichas respuestas pueden ser: evitar, aceptar, reducir o compartirlos. En la ejecución de este proceso, la dirección deberá considerar los efectos de probabilidad, impacto, costo – beneficio, entre otros; el riesgo final deberá estar alineado al riesgo aceptado y a la tolerancia al riesgo.

Actividades de control: corresponden a las políticas y procedimientos que se establecen para ayudar y llevar a cabo las respuestas a los riesgos que la dirección ha seleccionado. Las actividades de control combinan controles automatizados, manuales, de prevención, de detección, entre otras. Una actividad de control puede constituir una respuesta al riesgo por sí misma.

Información y comunicación: la información relevante respecto a la gestión de riesgos corporativos se debe identificar y comunicar en forma y plazos adecuados, esto permitirá al personal asumir adecuadamente sus responsabilidades. La comunicación de la gestión deberá provenir de la dirección, así como, ser clara y concisa a fin de garantizar el correcto entendimiento por todo el personal de la organización. Complementariamente, la entidad deberá implementar procesos y canales abiertos de comunicación que facilite su flujo en todas las direcciones (desde la dirección hacia

---

[21] El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 64).

[22] El riesgo residual es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 64).

todo el personal y viceversa, desde la organización hacia su entorno externo y viceversa).

Supervisión: es necesario supervisar constantemente los resultados de la gestión de riesgos corporativos a fin de garantizar la aplicación de correctivos oportunos cuando sea necesario. El proceso de supervisión puede ser llevada a cabo al interior de la organización (dirección, auditoría interna, etc.) o mediante el aporte independiente de terceros (auditoría externa, organismos de control, etc.). Resultado de la supervisión se obtendrá un informe de deficiencias[23].

Categorías de objetivos empresariales:

Estrategia: son objetivos de alto nivel que cada organización se fija para alcanzar su visión y misión.

Operaciones: son objetivos relacionados al uso eficaz y eficiente de los recursos de la entidad.

Información: estos objetivos buscan garantizar la fiabilidad de la información institucional.

Cumplimiento: son objetivos relativos a la aplicación obligatoria de leyes y normas.

---

[23] Una deficiencia es una situación dentro de la gestión de riesgos corporativos que merece atención y que puede representar una debilidad percibida, potencial o real, o una oportunidad para fortalecer la gestión de riesgos corporativos y aumentar la probabilidad de que se logren los objetivos de la entidad (COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 98).

1.6.3. TÉCNICAS DE IDENTIFICACIÓN DE RIESGOS

Las técnicas de identificación de riesgos conforme COSO ERM se deben llevar a cabo considerando tanto eventos del pasado (históricos) como del futuro, una forma sencilla es enfocarse en posibles acontecimientos derivados de percepciones del personal, en tanto que las técnicas más elaboradas estudian fuentes reales de eventos observables. Entre las principales técnicas el marco integrado de COSO ERM detalla a:

- Talleres interactivos de trabajo
- Entrevistas
- Cuestionarios
- Encuestas
- Reuniones de trabajo
- Análisis del flujo de procesos
- Rastreo de datos de eventos con pérdidas (empleo de archivos de datos sobre eventos individuales con pérdidas en el pasado)
- Inventario de eventos (acontecimientos potenciales comunes a empresas de un sector determinado)
- Indicadores de alarmas (uso de dispositivos de escala o umbral que generan alertas mediante la comparación de transacciones o eventos actuales con criterios predefinidos)
- Indicadores de eventos (supervisando datos correlacionados con los eventos importantes)
- Identificación continua de eventos (identificando la procedencia de la información y considerando los factores externos e internos que los pueden originar)

1.6.4. TÉCNICAS DE EVALUACIÓN DE RIESGOS

COSO ERM propone una metodología para la evaluación de riesgos de una entidad mediante una combinación de técnicas cualitativas y cuantitativas.

El marco integrado recomienda el uso de técnicas cualitativas cuando los riesgos identificados no se prestan a la cuantificación, cuando no se dispone de datos suficientes y creíbles para cuantificarlos, o, cuando el costo de la obtención y análisis resulta ineficaz. Por el contrario, las técnicas cuantitativas para la evaluación de riesgos requieren mayor esfuerzo y complejidad, ya que dependen de la calidad de los datos disponibles, para su efecto normalmente se emplea modelos matemáticos.

Entre las técnicas que detalla COSO ERM se encuentran a:

- Cuestionarios
- Entrevistas
- Talleres de trabajo
- Clasificación de riesgos
- Benchmarking
- Modelos probabilísticos (evaluación de valor en riesgo, flujo de caja en riesgo, beneficio en riesgo, valor de mercado en riesgo, distribuciones de pérdidas y análisis retrospectivos)
- Modelos no probabilísticos (análisis de sensibilidad, análisis de escenarios, pruebas de tolerancia a situaciones límite)
- Escalas de estimación

Complementariamente, COSO ERM expone métodos para presentar los resultados de las evaluaciones de riesgos tales como:

- Mapa de riesgo
- Mapa de calor
- Representaciones numéricas
- Visualización del riesgo al nivel de organización

1.6.5. TÉCNICAS DE TRATAMIENTO DE RIESGOS

A fin de dar tratamiento a los riesgos identificados como relevantes, COSO ERM propone las siguientes técnicas detalladas en el documento Gestión de Riesgos Corporativos – Marco Integrado – Técnicas de Aplicación:

- Análisis costo - beneficio
- Mirar los riesgos desde una perspectiva de cartera, es decir, mirar los riesgos de forma global o institucional
- Compartir los riesgos: por ejemplo, emplear contratación de seguros, acuerdos con terceros, externalización de una actividad
- Reducir los riesgos: por ejemplo, segregación funciones

1.7. ANÁLISIS Y DETERMINACIÓN DE ASPECTOS COMPLEMENTARIOS

En los puntos anteriores se ha analizado y plasmado en forma objetiva tanto la visión general y específica como las técnicas de identificación, evaluación y tratamiento de los riesgos propuestos por MAGERIT, ISO/IEC 27005 y COSO ERM, con esta base, se ha realizado un análisis comparativo a fin de determinar los aspectos relevantes de cada una y complementarios entre sí.

1.7.1. RELACIONADO AL ALCANCE

Las normas en forma general explican lo que se pretende obtener, sin embargo, no indican el cómo hacerlo, este es el caso de la norma ISO/IEC 27005 que en su texto indica: “Esta norma proporciona directrices para la gestión del riesgo de la seguridad de la información…. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo de la seguridad de la información. Corresponde a la organización definir

su enfoque para la gestión del riesgo…. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma"[24].

Las metodologías por su parte dan los lineamientos del cómo ejecutar los diferentes procesos y actividades, no obstante, muchas de las veces pueden estar mal dimensionadas a la realidad de una organización o no estar especializadas en un tema requerido, en este sentido, MAGERIT proporciona una metodología de análisis y gestión de riesgos orientada a sistemas de información (riesgos informáticos) y no a seguridad de la información.

Lo anterior está claramente descrito en el documento I – Método de MAGERIT que dice: "La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos"[25], complementariamente cita, "Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan"[26].

Dada la estrecha relación que tiene la "Información" con los sistemas automatizados y considerando la creciente dependencia que las organizaciones tienen en la tecnología, MAGERIT puede ser una guía bastante adaptable para gestionar los riesgos de la Información, sin embargo, es importante considerar adicionalmente que la Información no solo se procesa, transmite y reside en medios y sistemas automatizados, de hecho, la Información es manejada en procesos manuales, impresa y transmitida verbalmente incluso.

---

[24] NTEISO/IEC 27005 – Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información, introducción.

[25] MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, I - Método, página 6.

[26] Ídem

Por otra parte MAGERIT, no especifica de forma directa a qué tipo de organización (tamaño) está direccionada la metodología; conforme al análisis realizado, se puede inferir que su aplicabilidad directa se enfoca en grandes organizaciones, siendo pertinente adaptarla a instituciones medianas y pequeñas.

Los marcos de referencia, al igual que las normas, no puntualizan con exactitud el cómo abordar cada uno de los procesos y actividades que se deberían llevar a cabo. COSO ERM, brinda un marco de referencia integrado de la gestión de riesgos corporativos, enfocado al alineamiento del tratamiento de los riesgos con la estrategia y objetivos institucionales.

En conclusión, respecto al alcance de la norma, marco de referencia y metodología analizadas, se encuentra que existe un complemento interesante en el sentido de que MAGERIT es una metodología bien estructurada y estrechamente relacionada con la Información; por otra parte, en un proceso de riesgos de seguridad de la información, es indispensable considerar los objetivos estratégicos de la organización, tal como propone COSO ERM; en tanto que, ISO/IEC 27005 se centra específicamente en la gestión de riesgos de seguridad de la información.

1.7.2. RELACIONADO AL PROCESO

MAGERIT, plantea una metodología para la gestión de riesgos global muy sencilla y comprensible, ya que propone abarcar este reto como un proyecto con tres grandes procesos (planificación, análisis y gestión), sin embargo, en el desglose de sus actividades se torna algo compleja, sobre todo en el proceso de análisis de riesgos, que para su ejecución se debe identificar una serie de elementos, buscar dependencias e irlos ponderando en matrices con una notación muy técnica.

Al llevar a cabo las actividades conforme la metodología, es indispensable tener varios conceptos totalmente claros, por ejemplo, de las dimensiones

de seguridad, de elementos tecnológicos, entre otros; esta condición dificulta que el proceso sea llevado a cabo por personal no técnico, y hace necesario el apoyo de una herramienta automatizada.

Lo anterior se recoge en el documento I - Método de MAGERIT que dice: "Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte …. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar"[27].

La norma ISO/IEC 27005, propone un proceso global más completo que MAGERIT ya que incluye otros aspectos relevantes de gestión. La norma propone en términos generales dimensionar la gestión de riesgos, valorar los riesgos (identificar, estimar y evaluar), tratarlos, tomar decisiones, comunicar y hacer seguimiento. Corresponde a la organización y al equipo de trabajo, aplicar una metodología que ayude a transparentar los conceptos de gestión de riesgos a fin de que sea fácilmente entendida por personal no técnico al momento de llevar a cabo un proceso de análisis y evaluación de riesgos.

COSO ERM, plantea que la gestión de riesgos consta de ocho componentes relacionados entre sí, los mismos que no necesariamente deben ser ejecutados de forma secuencial "La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro"[28].

---

[27] MAGERIT v2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, I - Método, página 6.

[28] COSO ERM, Gestión de Riesgos Corporativos – Marco Integrado, página 18.

La estructura global que plantea el marco integrado de COSO ERM es muy similar a la propuesta por ISO/IEC 27005, teniendo que COSO ERM simplifica los procesos (componentes) de identificación de eventos y evaluación de riesgos respecto a la norma, ya que parte directamente de los eventos potenciales y los evalúa desde las perspectivas de probabilidad e impacto.

Complementariamente COSO ERM considera en todo su proceso tanto las amenazas como las oportunidades a fin de tratar las primeras y beneficiarse de las segundas.

En conclusión, se encuentra fortalezas en COSO ERM por su simplicidad en el proceso, sin embargo, la profundidad o alcance dentro de la organización que plantea este marco de referencia en la ejecución de los procesos de identificación, evaluación de los riesgos es global, es decir, se debe gestionar los riesgos de toda la organización, en tanto que ISO/IEC 27005 y MAGERIT recomiendan que se establezca un alcance, es decir, que se fijen límites para dicha gestión, lo cual puede ser más manejable en un proceso específico.

Un aporte importante de COSO ERM es la inclusión de identificación y tratamiento de las oportunidades en su proceso; la norma ISO/IEC 27005 de alguna manera también busca oportunidades de negocio al momento de dar tratamiento a los riesgos; en tanto que MAGERIT habla de oportunidades respecto a la pertinencia de ejecutar un proyecto de evaluación de riesgos.

1.7.3. RELACIONADO A LAS TÉCNICAS

La metodología de MAGERIT y el marco integrado de COSO ERM, proporcionan directamente las técnicas a utilizar en cada uno de sus procesos / componentes, constituyendo una fortaleza respecto a ISO/IEC

27005, adicionalmente, facilitan una guía de técnicas de aplicación en un documento complementario; por su parte, la norma ISO/IEC 27005 facilita guías de implementación del proceso de gestión de riesgos de seguridad de la información.

1.8. PREVISIONAMIENTO DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA CFN

Conforme el análisis realizado, a continuación se sintetiza en un cuadro comparativo los aspectos clave de la presente investigación que permitirán establecer una metodología de gestión de riesgos a la medida de la Corporación Financiera Nacional.

Tabla No 1.1: Previsionamiento de Metodología de Gestión de Riesgos de Seguridad de la Información

	MAGERIT	ISO/IEC 27005	COSO ERM	METODOLOGIA PARA CFN
Visión general (alcance)	Orientada a riesgos informáticos	Orientada a riesgos de seguridad de la información	Orientado a riesgos corporativos	Debería existir una sinergia entre ISO/IEC 27005 y COSO ERM, es decir, tratar los riesgos relacionados con la seguridad de la información considerando los riesgos corporativos (apoyo directo y visible a la consecución de objetivos institucionales)
Visión específica (involucrados)	Operativos y técnicos	Mandos altos y medios	Alta Gerencia	Debería involucrar a la Alta Gerencia para patrocinio, y, para el proceso de análisis y evaluación a los mandos altos (procurando que sean de carrera), acogiendo a ISO/IEC 27005 y COSO ERM
Visión específica (base de análisis)	Parte de identificar activos con un proceso técnico	Parte de identificar activos	Parte de identificar eventos positivos y negativos sobre objetivos organizacionales	La base para el análisis debería ser natural, combinar lo propuesto por ISO/IEC 27005 y COSO ERM, es decir, considerar a activos como parte fundamental de lo que se pretende proteger, y por otro identificar eventos, requerimientos y expectativas de seguridad

Visión específica (proceso)	Planificación: alcance y programación Análisis: activos, amenazas, salvaguardas, impacto, riesgo e interpretación de resultados (sobre dimensiones de seguridad) Gestión: Toma de decisiones, plan de	Contexto: criterios base, alcance Valoración: identificación (activos, amenazas, vulnerabilidades, consecuencias), estimación (valoración de consecuencias, incidentes, nivel de riesgo) y evaluación Tratamiento: controles, plan Aceptación Comunicación Monitoreo y Revisión	Ambiente Interno: filosofía y cultura Establecimiento objetivos Identificación eventos: positivos y negativos Evaluación: probabilidad e impacto Respuesta Actividades de Control: políticas, procedimientos, controles Información y comunicación	Se debería considerar a MAGERIT e ISO/IEC 27005 para contemplar una **planificación inicial** con el propósito de obtener el visto bueno de la Alta Gerencia y una programación macro, adicional acoger la definición de ISO/IEC 27005 referente a criterios base. El proceso macro debería ser simple (similar a MAGERIT) y contemplar **Análisis, Evaluación y Tratamiento de Riesgos** El análisis debería llegar hasta una identificación de riesgos, con base en dos pilares fundamentales como activos de información (tomado de MAGERIT e ISO/IEC 27005) y recolección de información del personal clave (COSO ERM); adicional contemplar tanto debilidades como oportunidades (COSO ERM) La evaluación de riesgos debería contemplar un proceso para lograr establecer el riesgo residual Sobre la base de todo lo anterior, el tratamiento de riesgos debería plasmarse en un plan de seguridad de largo plazo con las respectivas aprobaciones de los niveles más altos. Estas dos últimas (evaluación y tratamiento de riesgos),

	seguridad y ejecución		Supervisión	están contempladas en la norma, metodología y marco de referencia analizados
Técnicas	Diagramas: flujo de datos, de procesos Entrevistas Reuniones Presentaciones Valoración Delphi Arboles de ataque Análisis: mediante tablas, algorítmicos, costo-beneficio Gráficas:	No facilita técnicas directamente, sin embargo de las guías de implementación se puede deducir: Reuniones Entrevistas Encuestas Adicional suministra "tip's" importantes a considerar (ver sección 1.5.3, 1.3.4 y 1,5,5 del presente documento)	Talleres Entrevistas Cuestionarios Encuestas Reuniones de trabajo Análisis: flujo de trabajo, costo-beneficio Rastreo de datos Indicadores de: alarma, eventos Benchmarking Modelos probabilísticos Escalas de estimación	En relación a las técnicas que deberían aplicarse en una primera fase de gestión de riesgos destacan las **reuniones de trabajo** (COSO ERM) con personal clave (funcionarios del más alto nivel jerárquico, técnicos o responsables de aplicación/validación de controles), para facilitar y tener objetividad en el relevamiento de información se debería contar con registros claramente definidos (MAGERIT); en lo referente a la identificación de activos, vulnerabilidades, amenazas, probabilidad, impacto, controles, entre otros, se debería predefinir los criterios para su valoración mediante análisis de tablas (MAGERIT, ISO/IEC 27005) En todo el proceso es importante considerar los "tip's" de ISO/IEC 27005

	GANTT, histogramas, de Pareto y de tarta Planificación proyectos		Mapa de: riesgos, calor	

Elaborado por: *Tania Guevara H.*

Sobre la base de la tabla No. 1.1 en forma macro la Metodología de Gestión de Riesgos de Seguridad de la Información para CFN debería contemplar al menos:

- Planificación integral
- Análisis de riesgos
  - Determinación de activos
  - Relevamiento de información
  - Identificación de riesgos
- Evaluación de riesgos
  - Establecimiento de riesgo bruto
  - Identificación de controles existentes
  - Establecimiento de riesgo residual
- Tratamiento de riesgos

CAPITULO II. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2.1. INTRODUCCIÓN

La gestión de riesgos constituye un proceso esencial para organizar las iniciativas en materia de seguridad de la información, pues permiten conocer de manera objetiva el estado de seguridad, determinar la valoración del riesgo de la información y tomar las medidas de protección apropiadas.

Sobre la base de la norma, marco de referencia y metodología analizadas, considerando sus fortalezas y aspectos complementarios, se pretende desarrollar una metodología para la gestión de riesgos especializada en seguridad de la información, que sea aplicable a la Corporación Financiera Nacional – CFN, tendiente a apoyar a la consecución de los objetivos institucionales, de forma tal, de asegurar que los aspectos relevantes para la seguridad de la información se ejecutan controladamente.

2.2. OBJETIVOS

- Desarrollar una metodología para la gestión de riesgos que cuente con las siguientes características:

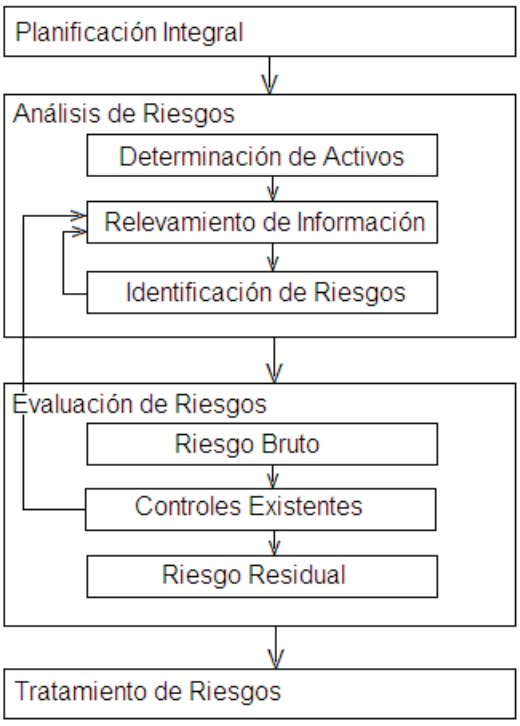
    - Especializada en seguridad de la información
    - Ajustado a las reales necesidades de la Corporación Financiera Nacional
    - De fácil despliegue y entendimiento para todo el personal de la CFN

2.3. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN FINANCIERA NACIONAL

2.3.1. ESTRUCTURACIÓN

La metodología que se propone para la Gestión de Riesgos de Seguridad de la Información para la Corporación Financiera Nacional consta de cuatro fases, cada una organizada en actividades y tareas. La figura 2.1, esquematiza la metodología propuesta.

Figura 2.1. Metodología de gestión de riesgos de la seguridad de la información para la Corporación Financiera Nacional



Elaborado: *Tania Guevara H.*

Para una adecuada gestión de riesgos, idealmente se busca contar con ciertas definiciones previas que soporten todo su proceso (ISO/IEC 27005), sin limitar a que las definiciones realizadas sean estáticas; la pertinencia

de revisión puede enmarcarse en un cambio de condiciones generales como por ejemplo, cambios en la misión o visión institucional, cambio en el giro del negocio, creación o eliminación productos de incidencia, etc.; por otro lado, puede ser conveniente validar las definiciones cuando han pasado estáticas en un tiempo razonable.

Mediante la fase de planificación integral, se organiza todo el trabajo obteniendo la aprobación y apoyo de la Dirección para iniciar el proceso y conseguir los recursos necesarios (MAGERIT e ISO/IEC 27005). En la fase de análisis de riesgos, se identifican las amenazas y vulnerabilidades sobre la fuente principal de entrevistas con funcionarios clave (COSO ERM) y activos de información (MAGERIT e ISO/IEC 27005), complementariamente, se recaba información pertinente conforme el alcance del análisis a realizar (COSE ERM e ISO/IEC 27005).

La evaluación de riesgos valora los escenarios de riesgo ponderando probabilidad e impacto, obteniendo de esta forma el riesgo bruto; seguido se evalúa los controles existentes a fin de determinar el riesgo residual (MAGERIT, ISO/IEC 27005 y COSO ERM). Finalmente, en la fase de tratamiento de riesgos, se elabora el plan de seguridad de la información que contiene los proyectos de seguridad encaminados a mitigar los riesgos de importancia que han sido identificados (MAGERIT, ISO/IEC 27005 y COSO ERM).

El monitoreo y la comunicación de riesgos son acciones esenciales para cerrar el ciclo de la gestión de riesgos, sin embargo, y considerando que los riesgos identificados son un input para la Gestión de Seguridad de la Información, dichas acciones formarán parte de referida gestión (ISO/IEC 27001).

2.3.2. VISIÓN GLOBAL

A continuación se sintetiza la metodología de gestión de riesgos de seguridad de la información propuesta para la Corporación Financiera Nacional:

Fase 1: Planificación integral
- Actividad A1.1: Planificación inicial
  - Tarea T1.1.1: Determinación del alcance
  - Tarea T1.1.2: Plan de trabajo de alto nivel
  - Tarea T1.1.3: Aprobación interna
  - Tarea T1.1.4: Conocimiento y aprobación de la Dirección
- Actividad A1.2: Planificación detallada
  - Tarea T1.2.1: Plan de trabajo detallado
  - Tarea T1.2.2: Aprobación interna del plan detallado
- Actividad A1.3: Lanzamiento del proceso
  - Tarea T1.3.1: Comunicación institucional

Fase 2: Análisis de riesgos
- Actividad A2.1: Determinación de activos
  - Tarea T2.1.1: Identificación de activos de información
  - Tarea T2.1.2: Valoración de activos de información
- Actividad A2.2: Relevamiento de información
  - Tarea T2.2.1: Entrevistas con el personal
  - Tarea T2.2.2: Recolección de documentación
- Actividad A2.3: Identificación de riesgos
  - Tarea T2.3.1: Identificación de vulnerabilidades
  - Tarea T2.3.2: Identificación de amenazas
  - Tarea T2.3.3: Estimación de probabilidad
  - Tarea T2.3.4: Estimación del impacto
- Actividad A2.4: Seguimiento de avance
  - Tarea T2.4.1: Informe de seguimiento de avance

Fase 3: Evaluación de riesgos

Actividad A3.1: Riesgo bruto

Tarea T3.1.1: Establecimiento de riesgo bruto

Actividad A3.2: Controles existentes

Tarea T3.2.1: Identificación de controles existentes

Tarea T3.2.1: Valoración de controles existentes

Actividad A3.3: Riesgo Residual

Tarea T3.1.1: Establecimiento de riesgo residual

Actividad A3.4: Seguimiento de avance

Tarea T3.4.1: Informe de seguimiento de avance

Fase 4: Tratamiento de riesgos

Actividad A4.1: Plan de Seguridad de la Información

Tarea T4.1.1: Formular Planes de Mitigación de los Riesgos

Tarea T4.1.2: Formular el Plan de Seguridad de la Información

Actividad A4.2: Aprobación interna

Tarea T4.2.1: Aprobación interna del Plan de Seguridad de la Información

Actividad A4.3: Aprobación de la Dirección

Tarea T4.3.1: Aprobación del Plan de Seguridad de la Información por parte del CAIR[29] y de la Dirección

2.3.3. FASE 1: PLANIFICACIÓN INTEGRAL

2.3.3.1. Actividad A1.1: Planificación inicial

La planificación inicial consta de las siguientes cuatro tareas:

Tarea T1.1.1: Determinación del alcance

Tarea T1.1.2: Plan de trabajo de alto nivel

Tarea T1.1.3: Aprobación interna

[29] CAIR – Comité de Administración Integral de Riesgos de la CFN

Tarea T1.1.4: Conocimiento y aprobación de la Dirección

Tabla No 2.1: Planificación inicial, Determinación del alcance

Fase 1: Planificación integral Actividad A1.1: Planificación inicial Tarea T1.1.1: Determinación del alcance
Objetivos • Determinar los procesos, productos o las áreas/unidades administrativas sobre los cuales se realizará el análisis y evaluación de riesgos de seguridad de la información • Determinar los recursos necesarios para la ejecución del análisis y evaluación de riesgos de seguridad de la información
Productos de entrada • Plan Estratégico Institucional CFN • Procesos • Organigrama CFN
Productos de salida • Especificación del alcance y límite de proceso de análisis y evaluación de riesgos de seguridad de la información • Requerimiento de recursos
Técnicas, prácticas y pautas • Reuniones de trabajo • Análisis de necesidad y oportunidad
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

Es indispensable delimitar el proceso de análisis y evaluación de riesgos (MAGERIT E ISO/IEC 27005) a fin de garantizar que el mismo se concluirá en un tiempo definido, caso contrario podría volverse una tarea sin fin y el

objetivo de todo el proceso es llegar a conclusiones específicas y objetivas sobre el estado de la seguridad en un determinado proceso, producto o área organizativa.

Complementariamente la definición de un alcance apoya directamente en el establecimiento de la pertinencia o no de ejecutar este proceso, y define los recursos tanto humanos como económicos que serán requeridos.

Tabla No 2.2: Planificación inicial, plan de trabajo de alto nivel

Fase 1: Planificación integral Actividad A1.1: Planificación inicial Tarea T1.1.2: Plan de trabajo de alto nivel
Objetivos • Planificar las entrevistas para el relevamiento de información • Definir las unidades organizacionales y funcionarios que intervendrán en el proceso
Productos de entrada • Resultados de la tarea T1.1.1 – Determinación del alcance
Productos de salida • Plan de entrevistas
Técnicas, prácticas y pautas • Reuniones de trabajo • Planificación de proyectos
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

El plan de entrevistas (MAGERIT y COSO ERM) servirá no sólo como parte de la planificación del proceso, sino también para coordinar los recursos (MAGERIT e ISO/IEC 27005) y programar las agendas del

personal involucrado tanto del negocio como personal técnico, con lo cual, cada área requerida podrá planificar su trabajo al interior de la misma.

Para la elaboración del orden de entrevistas deberá requerirse primero a funcionarios del negocio desde los niveles más gerenciales, continuando con funcionarios operativos para finalizar con personal de la Gerencia de División de Informática.

El orden recomendado se debe a que el negocio nos dará su input de requerimientos, vulnerabilidades y expectativas respecto a la seguridad de la información, mientras que los funcionarios administradores de la tecnología en su entrevista aparte de describir el funcionamiento, infraestructura y arquitectura de la tecnología, implícitamente irán explicando los diferentes controles existentes facilitando y acortando el tiempo en el hallazgo de vulnerabilidades y oportunidades.

Tabla No 2.3: Planificación inicial, aprobación interna

Fase 1: Planificación integral Actividad A1.1: Planificación inicial Tarea T1.1.3: Aprobación interna
Objetivos • Obtener el visto bueno de la Gerencia Nacional de Riesgos para la ejecución del proceso de análisis y evaluación de riesgos
Productos de entrada • Resultados de la tarea T1.1.1 – Determinación del alcance • Resultados de la tarea T1.1.2 – Plan de trabajo de alto nivel
Productos de salida • Aprobación por parte de la Gerencia Nacional de Riesgos • Especificación de alcance y límite definido • Plan de entrevistas depurado
Técnicas, prácticas y pautas • Reuniones de trabajo

• Correo electrónico • Memorandos
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática

Elaborado por: *Tania Guevara H.*

La aprobación interna permite el afinamiento del alcance, recursos y plan de entrevistas propuesto para el proceso de análisis y evaluación de riesgos de seguridad de la información.

Tabla No 2.4: Planificación inicial, conocimiento y aprobación de la Dirección

Fase 1: Planificación integral Actividad A1.1: Planificación inicial Tarea T1.1.4: Conocimiento y aprobación de la Dirección
Objetivos • Poner en conocimiento a la Dirección sobre el trabajo de análisis y evaluación de riesgos que se pretende emprender • Obtener el visto bueno y apoyo de la Dirección
Productos de entrada • Resultados de la tarea T1.1.3 - Aprobación interna
Productos de salida • Aprobación del proceso por parte de la Gerencia General de la CFN • Apoyo expreso para el arranque y ejecución del proceso
Técnicas, prácticas y pautas • Reuniones de trabajo • Presentaciones • Memorandos
Participantes • Gerente General

• Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática

Elaborado por: *Tania Guevara H.*

El visto bueno de la Dirección (MAGERIT, ISO/IEC 27005 y COSO ERM) constituye la declaración expresa de apoyo al proceso de análisis y evaluación de riesgos, y, su compromiso con la seguridad de la información. Este demanda por si solo la colaboración de los funcionarios involucrados y la asignación de los recursos correspondientes.

2.3.3.2. Actividad A1.2: Planificación detallada

Esta actividad consta de las siguientes tareas:

Tarea T1.2.1: Plan de trabajo detallado

Tarea T1.2.2: Aprobación interna del plan detallado

Tabla No 2.5: Planificación detallada, plan de trabajo detallado

Fase 1: Planificación integral Actividad A1.2: Planificación detallada Tarea T1.2.1: Plan de trabajo detallado
Objetivos • Complementar la planificación de alto nivel • Calendarizar todas las fases, actividades y tareas del proceso de análisis y evaluación de riesgos de seguridad de la información
Productos de entrada • Resultados de la tarea T1.1.3 - Aprobación interna • Resultados de la tarea T1.1.4: Conocimiento y aprobación de la Dirección • Metodología de gestión de riesgos de seguridad de la información (fases, actividades y tareas)

Productos de salida • Plan detallado del proceso (cronograma)
Técnicas, prácticas y pautas • Reuniones de trabajo • Planificación de proyectos
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

La planificación detallada del proceso de análisis y evaluación de riesgos de seguridad de la información entre otros aspectos determinará exactamente el tiempo demandante para su ejecución (MAGERIT).

Complementariamente definirá la profundidad del análisis y evaluación (MAGERIT e ISO/IEC 27005), es decir, en esta tarea quedará plasmada si se ejecutarán procesos adicionales que ayuden a corroborar o rectificar lo expresado por los funcionarios de negocio en el proceso de entrevistas, por ejemplo, se deberá definir si se realizarán análisis de vulnerabilidades, ethical hacking, revisiones presenciales en dispositivos de seguridad físicos en otras localidades (sucursales), entre otros.

Tabla No 2.6: Planificación detallada, aprobación interna del plan detallado

Fase 1: Planificación integral Actividad A1.2: Planificación detallada Tarea T1.2.2: Aprobación interna del plan detallado
Objetivos • Obtener el visto bueno de la Gerencia Nacional de Riesgos sobre el detalle del proceso
Productos de entrada • Resultados de la tarea T1.2.1 - Plan de trabajo detallado

Productos de salida • Aprobación por parte de la Gerencia Nacional de Riesgos • Plan detallado del proceso a ejecutar depurado (cronograma)
Técnicas, prácticas y pautas • Reuniones de trabajo • Correo electrónico • Memorandos
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática

Elaborado por: *Tania Guevara H.*

La aprobación del plan detallado posibilita una adecuada organización interna de las actividades diarias del Departamento Nacional de Seguridad Informática. Por su parte la Gerencia Nacional de Riesgos, estará permanentemente informada de los pormenores, lo cual permitirá una adecuada y oportuna comunicación con la Gerencia General en cuanto sea requerido (ISO/IEC 27005 y COSO ERM).

2.3.3.3. Actividad A1.3: Lanzamiento del proceso

El lanzamiento (MAGERIT) del análisis y evaluación de riesgos de seguridad de la información consta de la siguiente tarea:

Tarea T1.3.1: Comunicación institucional

Tabla No 2.7: Lanzamiento del proceso, comunicación institucional

Fase 1: Planificación integral Actividad A1.3: Lanzamiento del proceso Tarea T1.3.1: Comunicación institucional
Objetivos • Concienciar sobre la importancia de un proceso de análisis y evaluación de riesgos

• Informar a las diferentes áreas/unidades organizacionales involucradas sobre el proceso a iniciar y solicitar la debida cooperación
Productos de entrada • Resultados de la tarea T1.1.4: Conocimiento y aprobación de la Dirección • Resultados de la tarea T1.2.2: Aprobación interna del plan detallado
Productos de salida • Memorando informativo del trabajo a realizar
Técnicas, prácticas y pautas • Memorandos
Participantes • Gerente General • Gerente Nacional de Riesgos

Elaborado por: *Tania Guevara H.*

Mediante la ejecución de esta tarea se logra el apoyo y compromiso de las diferentes áreas / unidades organizacionales; de ser el caso, complementariamente cada una de éstas podrá reorganizar su trabajo interno.

2.3.4. FASE 2: ANÁLISIS DE RIESGOS

2.3.4.1. Actividad A2.1: Determinación de activos

La determinación de activos (MAGERIT e ISO/IEC 27005) consta de las siguientes tareas:

Tarea T2.1.1: Identificación de activos de información

Tarea T2.1.2: Valoración de activos de información

Tabla No 2.8: Determinación de activos, identificación

Fase 2: Análisis de riesgos Actividad A2.1: Determinación de activos Tarea T2.1.1: Identificación de activos de información
Objetivos • Identificar los activos de información que forman parte en el alcance definido para el proceso de análisis y evaluación de riesgos de seguridad de la información
Productos de entrada • Listado de procesos y registros del Sistema de Calidad de la CFN • Política para información institucional[30] • Inventarios de datos de negocio y tecnológicos
Productos de salida • Inventario de activos de información clasificados por el Propietario de la Información[31]
Técnicas, prácticas y pautas • Entrevistas • Reuniones de Trabajo • Correo electrónico • Memorandos
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

[30] La Política para Información Institucional, se basa en las normas y políticas de Seguridad de la Información de la CFN y la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP; su objetivo primordial es normar el manejo de la información institucional en función de su grado de sensitividad.

[31] El término "propietario" se refiere al funcionario al cual se le ha asignado la responsabilidad administrativa para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona tenga realmente algún derecho de propiedad sobre el activo de información (Política de Seguridad de la Información CFN, página 2).

• Propietarios de la Información • Analistas de Desarrollo Organizacional

Elaborado por: *Tania Guevara H.*

El inventario de activos de información deberá tener la siguiente información:

- Identificación del activo (código)
- Nombre del activo de información
- Código del procedimiento[32]
- Nombre del procedimiento
- Área/Unidad que custodia del activo
- Breve detalle del contenido de la información
- Área responsable del activo

Tabla No 2.9: Determinación de activos, valoración

Fase 2: Análisis de riesgos Actividad A2.1: Determinación de activos Tarea T2.1.2: Valoración de activos de información
Objetivos • Identificar el grado de confidencialidad, integridad y disponibilidad que tiene el activo de información
Productos de entrada • Resultados de la tarea T2.1.1: Identificación de activos de información • Norma de Seguridad de la Información relacionada a la Gestión de Activos • Procedimiento para clasificación de la información SI-26
Productos de salida

[32] Código y nombre del procedimiento, aplicable a la clasificación de la información por el grado de sensitividad.

• Listado índice temático de información reservada • Clasificación de la información por el grado de sensitividad
Técnicas, prácticas y pautas • Entrevistas • Reuniones de trabajo • Correo electrónico • Memorandos
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática • Propietarios de la Información

Elaborado por: *Tania Guevara H.*

La valoración de activos de información permite conocer la importancia del activo en términos de valor para la institución, lo cual permite dar un tratamiento y protección acordes a los requerimientos de negocio (MAGERIT e ISO/IEC 27005).

2.3.4.2. Actividad A2.2: Relevamiento de información

Consta de las siguientes tareas:

Tarea T2.2.1: Entrevistas con el personal

Tarea T2.2.2: Recolección de documentación

Tabla No 2.10: Relevamiento de información, entrevistas

Fase 2: Análisis de riesgos Actividad A2.2: Relevamiento de información Tarea T2.2.1: Entrevistas con el personal
Objetivos • Recabar las preocupaciones y expectativas del negocio para lograr los objetivos institucionales, relacionada con aspectos relevantes

de seguridad de la información previamente definidos, sobre los cuales interesa identificar tanto vulnerabilidades como oportunidades • Recabar información de funcionarios técnicos y otros encargados de la administración de controles
Productos de entrada • Anexo A - Registro de Levantamiento de Información (formato)
Productos de salida • Anexo A - Registro de Levantamiento de Información (con información proporcionada por el funcionario entrevistado) • Acta de reunión
Técnicas, prácticas y pautas • Reuniones de trabajo • Entrevistas - cuestionarios • Técnicas de observación
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática • Propietarios de la información • Funcionarios técnicos de la Gerencia de División de Informática y otros encargados de la administración de controles • Funcionarios que proporcionan información útil en la identificación de vulnerabilidades, controles y oportunidades

Elaborado por: *Tania Guevara H.*

La tarea de entrevistas es una de las más sensibles del proceso ya que es la fuente de información base para detectar las vulnerabilidades y finalmente riesgos a las que está expuesta la información (MAGERIT y COSO ERM), también constituye un input importante para descubrir las oportunidades de mejoramiento y controles en aspectos de importancia para la seguridad de la información.

Por lo anterior, los funcionarios seleccionados para esta tarea deben tener un amplio conocimiento del negocio, proceso o producto que se está analizando, en forma ideal, deberían ser los propietarios de la información o los funcionarios responsables de las áreas/unidades organizacionales.

El formato del Anexo A contiene los aspectos considerados como relevantes relacionados con la seguridad de la información, éste deberá ser revisado y redimensionado dependiendo del alcance del proceso de análisis y evaluación de riesgos que se vaya a ejecutar.

Tabla No 2.11: Relevamiento de información, recolección de documentación

Fase 2: Análisis de riesgos Actividad A2.2: Relevamiento de información Tarea T2.2.2: Recolección de documentación
Objetivos • Identificar y recabar información importante y documentada que forme parte del alcance del proceso de análisis y evaluación de riesgos de seguridad de la información • Complementar la información obtenida de los funcionarios en las entrevistas, tarea T2.2.1: Entrevistas con el personal
Productos de entrada • Información institucional documentada • Políticas, Normas, Manuales, Procesos, Procedimientos, entre otros del Sistema de Calidad
Productos de salida • Material de soporte para hallazgo de vulnerabilidades, controles y oportunidades
Técnicas, prácticas y pautas • No aplica
Participantes • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

El recabar información adicional ayudará comprender de mejor manera lo expuesto por los funcionarios entrevistados (ISO/IEC 27005 y COSO ERM), constituye una fuente para contrastar y/o confirmar la información obtenida en la tarea de entrevistas.

2.3.4.3. Actividad A2.3: Identificación de riesgos

La identificación de riesgos consta de las siguientes cuatro tareas:

Tarea T2.3.1: Identificación de vulnerabilidades

Tarea T2.3.2: Identificación de amenazas

Tarea T2.3.3: Estimación de probabilidad

Tarea T2.3.4: Estimación del impacto

Tabla No 2.12: Identificación de riesgos, identificación de vulnerabilidades

Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.1: Identificación de vulnerabilidades
Objetivos • Identificar las fallas o insuficiencias presentes en la organización, procesos (de gestión, negocio, técnicos, etc.), ambiente físico, sistemas informáticos y sus soportes, entre otros. • Relacionar las vulnerabilidades identificadas con los aspectos relevantes de seguridad definidos
Productos de entrada • Resultados de la tarea T2.2.1: Entrevistas con el personal • Resultados de la tarea T2.2.2: Recolección de documentación
Productos de salida • Lista de vulnerabilidades agrupadas por aspectos relevantes de seguridad de la información
Técnicas, prácticas y pautas • Reuniones de trabajo

• Entrevistas • Revisión y análisis de documentación • Análisis de vulnerabilidades • Ethical Hancking
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

En esta tarea se debe analizar cuidadosamente la información levantada en las entrevistas a fin de identificar hechos que constituirían un escenario de riesgo para la información; complementariamente, se debe revisar la documentación adicional recolectada con lo cual se irá concluyendo sobre las vulnerabilidades existentes en los diferentes procesos, áreas/unidades organizacionales o productos conforme el alcance del proceso de análisis y evaluación de riesgos. Paralelamente se identificará oportunidades de mejora, sin embargo, el principal objetivo es identificar vulnerabilidades (COSO ERM).

Para la identificación tanto de vulnerabilidades como de oportunidades, influirá el conocimiento y experiencia sobre procesos del negocio y técnicos institucionales que posea el personal que está a cargo de analizar la información recolectada, sin embargo, es recomendable no dejar de lado ningún aspecto por trivial que luzca a fin de no inyectar subjetividad en el proceso.

Tabla No 2.13: Identificación de riesgos, identificación de amenazas

Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.2: Identificación de amenazas

Objetivos • Identificar las amenazas significativas que podrían materializarse dada la existencia de una vulnerabilidad
Productos de entrada • Anexo B – Catálogo de Amenazas • Resultados de la tarea T2.3.1: Identificación de vulnerabilidades
Productos de salida • Listado de amenazas relacionadas a las vulnerabilidades y aspectos relevantes de seguridad de la información
Técnicas, prácticas y pautas • Catálogo de amenazas (Anexo B) • Reuniones de trabajo • Valoración Delphi
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

A fin de que la identificación de amenazas sea lo más realista posible, se deberá considerar tanto la experiencia propia de la CFN (historial) como de la de los sectores financiero y público (MAGERIT, ISO/IEC 27005 y COSO ERM).

Tabla No 2.14: Identificación de riesgos, estimación de probabilidad

Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.3: Estimación de probabilidad
Objetivos • Estimar cualitativamente la posibilidad (frecuencia) de que ocurra una amenaza dada una vulnerabilidad
Productos de entrada • Resultados de la tarea T2.3.1: Identificación de vulnerabilidades

• Resultados de la tarea T2.3.2: Identificación de amenazas • Anexo C - Criterios para Calificar la Probabilidad de Ocurrencia
Productos de salida • Una lista de probabilidades de ocurrencia valoradas
Técnicas, prácticas y pautas • Criterios de probabilidad (Anexo C) • Reuniones de trabajo • Valoración Delphi
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

La estimación de la probabilidad se la realiza en base de la aplicación de los criterios predefinidos Anexo C (MAGERIT, ISO/IEC 27005 y COSO ERM).

Tabla No 2.15: Identificación de riesgos, estimación del impacto

Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.4: Estimación del impacto
Objetivos • Estimar cualitativamente el daño potencial (afectación) que puede tener la información y el negocio en caso de explotar una amenaza sobre una vulnerabilidad
Productos de entrada • Resultados de la tarea T2.3.1: Identificación de vulnerabilidades • Resultados de la tarea T2.3.2: Identificación de amenazas • Anexo D - Criterios para Calificar el Nivel de Impacto
Productos de salida • Una lista de impactos valorados

Técnicas, prácticas y pautas • Criterios del nivel de impacto (Anexo D) • Reuniones de trabajo • Valoración Delphi
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

La estimación del impacto se la realiza en base de la aplicación de los criterios predefinidos Anexo D (MAGERIT, ISO/IEC 27005 y COSO ERM).

2.3.4.4. Actividad A2.4: Seguimiento de avance

Esta actividad consta de la única tarea:

Tarea T2.4.1: Informe de seguimiento de avance

Tabla No 2.16: Análisis de riesgos, informe de seguimiento de avance

Fase 2: Análisis de riesgos Actividad A2.4: Seguimiento de avance Tarea T2.4.1: Informe de seguimiento de avance
Objetivos • Asegurar que el proceso de análisis y evaluación de riesgos de seguridad de la información se ejecuta dentro del cronograma establecido y con los recursos conforme la planificación
Productos de entrada • Resultados de la actividad A2.1: Determinación de activos • Resultados de la actividad A2.2: Relevamiento de información • Resultados de la actividad A2.3: Identificación de riesgos
Productos de salida • Informe de seguimiento de avance

Técnicas, prácticas y pautas • No aplica
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

2.3.5. FASE 3: EVALUACIÓN DE RIESGOS

2.3.5.1. Actividad A3.1: Riesgo bruto

Consta de la siguiente tarea:

Tarea T3.1.1: Establecimiento de riesgo bruto

Tabla No 2.17: Riesgo bruto, establecimiento

Fase 3: Evaluación de riesgos Actividad A3.1: Riesgo bruto Tarea T3.1.1: Establecimiento de riesgo bruto
Objetivos • Determinar el riesgo bruto analizando el impacto ponderado por la frecuencia o probabilidad de ocurrencia de la amenaza
Productos de entrada • Resultados de la fase 2 - Análisis de riesgos (amenaza, vulnerabilidad, probabilidad e impacto) • Anexo E – Criterios para Calificar el Riesgo Bruto
Productos de salida • Una lista de riesgos brutos valorados
Técnicas, prácticas y pautas • Análisis mediante tablas

Participantes
• Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

El riesgo bruto constituye la exposición total al riesgo, sin considerar los controles existentes, en primera instancia se propone una evaluación cualitativa, sin embargo, para futuros procesos de análisis y evaluación de riesgos se recomienda aplicar una valoración cuantitativa, la misma que será posible siempre y cuando se cuente con un conocimiento suficiente de los costos que tengan los incidentes de seguridad de la información (MAGERIT, ISO/IEC 27005 y COSO ERM).

2.3.5.2. Actividad A3.2: Controles existentes

Consta de las siguientes tareas:

Tarea T3.2.1: Identificación de controles existentes

Tarea T3.2.1: Valoración de controles existentes

Tabla No 2.18: Controles existentes, identificación

Fase 3: Evaluación de riesgos Actividad A3.2: Controles existentes Tarea T3.2.1: Identificación de controles existentes
Objetivos • Identificar los controles previstos e implementados
Productos de entrada • Resultados de la tarea T2.2.1: Entrevistas con el personal • Resultados de la tarea T2.2.2: Recolección de documentación
Productos de salida • Un listado de controles previstos e implementados
Técnicas, prácticas y pautas • Reuniones de trabajo

• Entrevistas • Revisión de documentación
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática • Funcionarios técnicos y encargados de la administración de controles

Elaborado por: *Tania Guevara H.*

En la ejecución de esta tarea se deberá considerar a todo tipo de controles sean preventivos, detectivos, manuales, automáticos, administrativos, técnicos, etc. (MAGERIT, ISO/IEC 27005 y COSO ERM); para los cuales es importante documentar los siguientes atributos:

- Nombre: un nombre descriptivo del control
- Responsable: cargo del funcionario principal y/o delegado
- Tipo: preventivo / detectivo
- Naturaleza: manual / automático
- Frecuencia: constante, diario, semanal, quincenal, mensual, trimestral, semestral, anual
- Funcionamiento del control: si el control está operativo o no
- Observaciones de auditoria: si existe abierta una observación de auditoria interna, externa o de organismos de control

Tabla No 2.19: Controles existentes, valoración

Fase 3: Evaluación de riesgos Actividad A3.2: Controles existentes Tarea T3.2.1: Valoración de controles existentes
Objetivos • Determinar la eficacia de los controles implementados
Productos de entrada • Resultados de la tarea T3.2.1: Identificación de controles existentes

• Resultados de la tarea T2.2.1: Entrevistas con el personal • Resultados de la tarea T2.2.2: Recolección de documentación • Anexo F – Criterios para Calificar la Eficacia de Controles
Productos de salida • Una lista de controles existentes valorados
Técnicas, prácticas y pautas • Reuniones de trabajo • Entrevistas • Revisión de documentación • Análisis de tablas • Valoración Delphi
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática • Funcionarios técnicos, encargados de la administración de controles y de verificación del cumplimiento

Elaborado por: *Tania Guevara H.*

Para el establecimiento de la eficacia del control evaluado se consideraran los criterios definidos en el Anexo F (MAGERIT), en términos generales tenemos tres categorías:

- Fuerte: corresponde a un control implementado que logra el objetivo de mitigar el riesgo
- Moderado: corresponde a un control implementado que logra parcialmente el objetivo de mitigar el riesgo
- Débil: corresponde a un control implementado que por cualquier motivo dejó de cumplir con el objetivo de mitigar el riesgo

2.3.5.3. Actividad A3.3: Riesgo Residual

Consta de la siguiente tarea:

Tarea T3.1.1: Establecimiento de riesgo residual

Tabla No 2.20: Riesgo Residual, establecimiento

Fase 3: Evaluación de riesgos Actividad A3.3: Riesgo Residual Tarea T3.1.1: Establecimiento de riesgo residual
Objetivos • Determinar el riesgo residual analizando la eficacia de los controles previstos e implementados
Productos de entrada • Resultados de la tarea T3.1.1: Establecimiento de riesgo bruto • Resultados de la tarea T3.2.1: Valoración de controles existentes • Anexo G – Criterios para Calificar el Riesgo Residual
Productos de salida • Una lista de riesgos residuales valorados
Técnicas, prácticas y pautas • Análisis mediante tablas
Participantes • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

El riesgo residual es la exposición total al riesgo tomando en cuenta los controles previstos e implementados (MAGERIT, ISO/IEC 27005 y COSO ERM), al igual que en la tarea T3.1.1: Establecimiento de riesgo bruto, se recomienda iniciar con valoraciones cualitativas para luego pasar a valorar el riesgo cuantitativamente.

2.3.5.4. Actividad A3.4: Seguimiento de avance

Esta actividad consta de la única tarea:

Tarea T3.4.1: Informe de seguimiento de avance

Tabla No 2.21: Evaluación de riesgos, Informe de seguimiento de avance

Fase 3: Evaluación de riesgos Actividad A3.4: Seguimiento de avance Tarea T3.4.1: Informe de seguimiento de avance
Objetivos • Asegurar que el proceso de análisis y evaluación de riesgos de seguridad de la información se ejecuta dentro del cronograma establecido y con los recursos conforme la planificación
Productos de entrada • Resultados de la actividad A3.1: Riesgo bruto • Resultados de la actividad A3.2: Controles existentes • Resultados de la actividad A3.3: Riesgo Residual
Productos de salida • Informe de seguimiento de avance
Técnicas, prácticas y pautas • No aplica
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática

Elaborado por: *Tania Guevara H.*

2.3.6. FASE 4: TRATAMIENTO DE RIESGOS

2.3.6.1. Actividad A4.1: Plan de Seguridad de la Información

Esta actividad consta de las siguientes tareas:

Tarea T4.1.1: Formular Planes de Mitigación de los Riesgos

Tarea T4.1.2: Formular el Plan de Seguridad de la Información

Tabla No 2.22: Plan de seguridad de la información, planes de mitigación

Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información Tarea T4.1.1: Formular Planes de Mitigación de los Riesgos
Objetivos • Elaborar varias recomendaciones que servirán para mitigar los riesgos identificados
Productos de entrada • Resultados de la fase 3: Evaluación de riesgos
Productos de salida • Una lista de planes para mitigar los riesgos
Técnicas, prácticas y pautas • Reuniones de trabajo • Análisis costo – beneficio
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática • Funcionarios técnicos • Funcionarios de negocio

Elaborado por: *Tania Guevara H.*

Los planes de mitigación de riesgos no constituyen un proyecto en sí, más bien está orientado a describir las recomendaciones o acciones a seguir para superar los riesgos (MAGERIT).

Es importante la participación parcial de especialistas técnicos y de negocio debido a que la ejecución e implementación de los planes de mitigación no todos son de responsabilidad del Área de Seguridad Informática y se requiere del consenso de los responsables.

Tabla No 2.23: Plan de seguridad de la información, formular el plan

Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información Tarea T4.1.2: Formular el Plan de Seguridad de la Información
Objetivos • Elaborar un plan de alto nivel de seguridad de la información • Organizar y agrupar los planes de mitigación en proyectos de seguridad de la información • Priorizar los proyectos de seguridad de la información
Productos de entrada • Resultados de la tarea T4.1.1: Formular Planes de Mitigación de los Riesgos
Productos de salida • Plan de Seguridad de la Información
Técnicas, prácticas y pautas • Reuniones de trabajo • Análisis costo – beneficio • Planificación de proyectos
Participantes • Jefe Nacional de Seguridad Informática • Analistas de Seguridad Informática • Funcionarios técnicos • Funcionarios de negocio

Elaborado por: *Tania Guevara H.*

En la elaboración del Plan de Seguridad de la Información (MAGERIT, ISO/IEC 27005 y COSO ERM) se deberá considerar siempre a los riesgos calificados como superior y alto, sin que quede restringido el tratamiento para los riesgos moderados o de menor calificación.

La participación parcial de especialistas técnicos y de negocio ayudará en el proceso de priorización y calendarización de los proyectos que formarán parte del plan de seguridad.

2.3.6.2. Actividad A4.2: Aprobación interna

Consta de la siguiente tarea:

Tarea T4.2.1: Aprobación interna del Plan de Seguridad de la Información

Tabla No 2.24: Aprobación interna, del plan de seguridad

Fase 4: Tratamiento de riesgos Actividad A4.2: Aprobación interna Tarea T4.2.1: Aprobación interna del Plan de Seguridad de la Información
Objetivos • Obtener el visto bueno de la Gerencia Nacional de Riesgos respecto al Plan de Seguridad de la Información
Productos de entrada • Resultados de la tarea T4.1.2: Formular el Plan de Seguridad de la Información
Productos de salida • Plan de Seguridad de la Información aprobado por la Gerencia Nacional de Riesgos
Técnicas, prácticas y pautas • Reuniones de trabajo • Correo electrónico • Memorandos
Participantes • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad Informática

Elaborado por: *Tania Guevara H.*

2.3.6.3. Actividad A4.3: Aprobación de la Dirección

Consta de la siguiente tarea (MAGERIT, ISO/IEC 27005 y COSO ERM):

Tarea T4.3.1: Aprobación del Plan de Seguridad de la Información por parte del CAIR y de la Dirección

Tabla No 2.25: Aprobación de la Dirección, del plan de seguridad

Fase 4: Tratamiento de riesgos Actividad A4.3: Aprobación de la Dirección Tarea T4.3.1: Aprobación del Plan de Seguridad de la Información por parte del CAIR y de la Dirección
Objetivos • Poner en conocimiento del CAIR sobre los resultados del trabajo realizado • Que el CAIR recomiende la aprobación del Plan de Seguridad de la Información al Gerente General • Obtener la aprobación del Plan por parte del Gerente General de la CFN
Productos de entrada • Aprobación interna del Plan de Seguridad de la Información
Productos de salida • Plan de Seguridad de la Información aprobado
Técnicas, prácticas y pautas • Presentaciones • Reuniones de Trabajo • Memorandos
Participantes • Gerente General • CAIR – Comité de Administración Integral de Riesgos • Gerente Nacional de Riesgos • Jefe Nacional de Seguridad de la Información

Elaborado por: *Tania Guevara H.*

CAPITULO III. EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. INTRODUCCIÓN

En este capítulo se realizará un diagnóstico de la situación actual de la Corporación Financiera Nacional en materia de seguridad mediante una evaluación de riesgos de seguridad de la información aplicada a los procesos de negocio de la CFN, los resultados de la evaluación servirán de insumo para el diseño del Modelo de Gestión de Seguridad.

3.2. OBJETIVO

- Realizar una Evaluación de Riesgos de Seguridad de la Información en la Corporación Financiera Nacional aplicando la metodología propuesta en el capítulo anterior.

3.3. APLICACIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CFN

A continuación se describe el desarrollo del análisis y evaluación de riesgos de seguridad de la información realizada en la Corporación Financiera Nacional, y se adjunta los resultados de la misma.

3.3.1. FASE 1: PLANIFICACIÓN INTEGRAL

3.3.1.1. Actividad A1.1: Planificación inicial

Para los detalles de esta actividad, ver sección 2.3.3.1

3.3.1.1.1. Tarea T1.1.1: Determinación del alcance

3.3.1.1.2. Tarea T1.1.2: Plan de trabajo de alto nivel

Tabla No 3.1: Acta de reunión, plan de trabajo de alto nivel

Acta de Reunión

Fecha**:** Lunes, 15 de Agosto del 2011

Participantes

Xxxxx Xxxxxx	Jefe Nacional de Seguridad Informática
Xxxxx Xxxxxx	Analista de Seguridad Informática

Asunto: Proyecto Evaluación de Riesgos de Seguridad de la Información

Temas tratados

- Presentación del proyecto, el responsable del Área de Seguridad, expone los objetivos de realizar un análisis y evaluación de riesgos de seguridad de la información
- El grupo de trabajo determina que es oportuno y conveniente llevar a cabo el proyecto propuesto, ya que se permitirá conocer de manera objetiva el estado de la seguridad y viabilizará la ejecución ordenada y priorizada de proyectos para apoyar los objetivos institucionales
- Se determina como alcance al proceso primordial del negocio "Concesión de Crédito" que involucra a créditos de Primer Piso, Segundo Piso, Transporte y Comercio Exterior, adicionalmente, y considerando que los objetivos básicos de seguridad de la información son garantizar la confidencialidad, integridad y disponibilidad de la misma, los aspectos relevantes (dominios) a los que se enfocará el presente análisis serán 2.2.1 Política de Seguridad, 2.2.4. Seguridad Ligada a los Recursos Humano, 2.2.6. Gestión de Comunicaciones y Operaciones, y, 2.2.7. Control de Accesos
- Se elabora un borrador del cronograma de talleres (entrevistas) para relevamiento de información con los propietarios de información y funcionarios responsables de áreas de negocio y técnicas

Resultados – anexos: Plan de entrevistas.

Firma de los participantes

Xxxxx Xxxxxx Jefe Nal. de Seguridad Informática	Xxxxx Xxxxxx Analista Seguridad Informática

Elaborado por: *Tania Guevara H.*

Tabla No 3.2: Plan de entrevistas

Agenda Reuniones	Num. Horas
Gerente de División de Fomento y Crédito	1
Gerente de División de Comercio Exterior	2
Gerente Nacional de Concesión de Crédito	2
Subgerente Nacional de Crédito de Primer Piso	3
Subgerente Nal. de Crédito de Segundo Piso	2
Subgerente Nal de Transporte y Prog. Especiales	2
Subgerente Nal. De Recursos Humanos y DO	2
Gerente Nal. de Coord. de Oficinas y Ventanillas	1
Auditor Interno	2
Subgerente Nacional de Auditoria Informática	2
Gerente de División de Informática	2
Subgerente Nal. de Implementación de Sistemas	5
Subgerente Nacional de Atención al Usuario	2
Subgerente Nacional de Producción y Control	2
Subgerente Nacional de Infraestructura de TI	2
Gerente y Gerencias Sucursal Mayor	3
Subgerente Regional de Informática	5
Gerente Sucursal Ambato	6

Elaborado por: *Tania Guevara H.*

3.3.1.1.3. Tarea T1.1.3: Aprobación interna

Tabla No 3.3: Acta de Reunión, aprobación interna

Acta de Reunión

Fecha: Martes, 16 de Agosto del 2011

Participantes

Xxxxx Xxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxx	Jefe Nacional de Seguridad Informática

Asunto: Presentación y aprobación interna del proyecto de evaluación de riesgos de seguridad de la información

Temas tratados

- Presentación interna del proyecto por parte del Jefe de Seguridad Informática
  - Revisión de los objetivos del proyecto
  - Revisión del alcance
  - Factores críticos de éxito
  - Revisión del cronograma de entrevistas
- La Gerencia Nacional de Riesgos, ratifica y aprueba el alcance definido y el cronograma para entrevistas
- Se elabora un memorando para poner en conocimiento y solicitar la aprobación a la Gerencia General para la ejecución del proyecto de análisis y evaluación de riesgos de seguridad de la información

Resultados – anexos

Memorando para aprobación del proyecto.

Firma de los participantes

Xxxxx Xxxxxx Gerente Nacional de Riesgos	Xxxxx Xxxxxx Jefe Nal. de Seguridad Informática

Elaborado por: *Tania Guevara H.*

MEMORANDO

SI – XXXX1

PARA: Xxxxx Xxxxxx
Gerente General

C.C: Xxxxx Xxxxxx
Subgerente General

DE: Xxxxx Xxxxxx
Gerente Nacional de Riesgos

ASUNTO: Proyecto Evaluación de Riesgos de Seguridad de la Información

FECHA: Quito, 17 de Agosto del 2011

Antecedentes

La Superintendencia de Bancos y Seguros con resolución de Junta Bancaria No. JB-2005-834 del 20 de octubre del 2005 dispone a las entidades controladas identificar los requerimientos de seguridad relacionados con la tecnología de información, considerando la evaluación de los riesgos que enfrenta la institución y un plan para evaluar el desempeño del sistema de administración de seguridad de la información.

Las Políticas de Seguridad de la Información aprobadas por el Directorio de la CFN con resolución No. DIR-2009-198 del 24 de diciembre del 2009 demandan el análisis de riesgos y un programa de seguridad de la información.

El análisis y la gestión de riesgos de la información constituyen tareas esenciales para organizas las iniciativas en materia de seguridad de la información, pues permiten conocer de manera objetiva el estado de seguridad, determinar la

valoración del riesgo de la información y tomar las medidas de protección apropiadas.

Justificativo

Conforme los antecedentes expuestos, la CFN requiere disponer de un Plan de Seguridad de la Información que permita a la entidad tomar acción sobre posibles falencias de seguridad identificadas en base a un análisis y evaluación de riesgos.

Adicionalmente, la planificación del Departamento Nacional de Seguridad Informática contempla el Proyecto de Evaluación de Riesgos de Seguridad de la Información, cuyo objetivo principal es diseñar y formular el Plan de Seguridad de la Información a largo plazo, tendiente a incrementar la confidencialidad, integridad y disponibilidad; el control de los sistemas informáticos y de la información a fin de apoyar la continuidad del negocio. Estas actividades permitirán además, determinar los riesgos, proteger los bienes y servicios informáticos, así como, la información sensible de la Corporación Financiera Nacional.

Solicitud

Con los antecedentes y justificación expuestos, solicitamos su aprobación para el desarrollo del Proyecto “Evaluación de Riesgos de Seguridad de la Información”, planteado conforme el siguiente cronograma macro de trabajo, con inicio en agosto del 2011:

Fase	**Tiempo (días)**
Fase I – Planificación Integral	5
Fase II – Análisis de Riesgos	20
Fase III – Evaluación de Riesgos	5
Fase IV – Tratamiento de Riesgos	10

Los factores de éxito para la evaluación efectiva de riesgos de seguridad de la información son:

- Compromiso de la Gerencia General y Gerencias, para la ejecución efectiva del proyecto
- Realización de las entrevistas en las fechas y horas planificadas, para que no causen retraso al proyecto
- Conocimiento de los entrevistados de los procesos del área que manejan
- Entrega oportuna de la información de los procesos evaluados
- Indicar con claridad los riesgos de seguridad detectados
- Que las áreas involucradas tengan claro el objetivo a conseguir

Atentamente,

Xxxxx Xxxxxx	Xxxxx Xxxxxx
Jefe Nal de Seguridad Informática	Gerente Nacional de Riesgos

c.c. Archivo General

3.3.1.1.4. Tarea T1.1.4: Conocimiento y aprobación de la Dirección

Mediante sello y firma inscrita en memorando SI-XXXX1, la Gerencia General aprueba y respalda la ejecución del proyecto Evaluación de Riesgos de Seguridad de la Información conforme lo propuesto por la Gerencia Nacional de Riesgos.

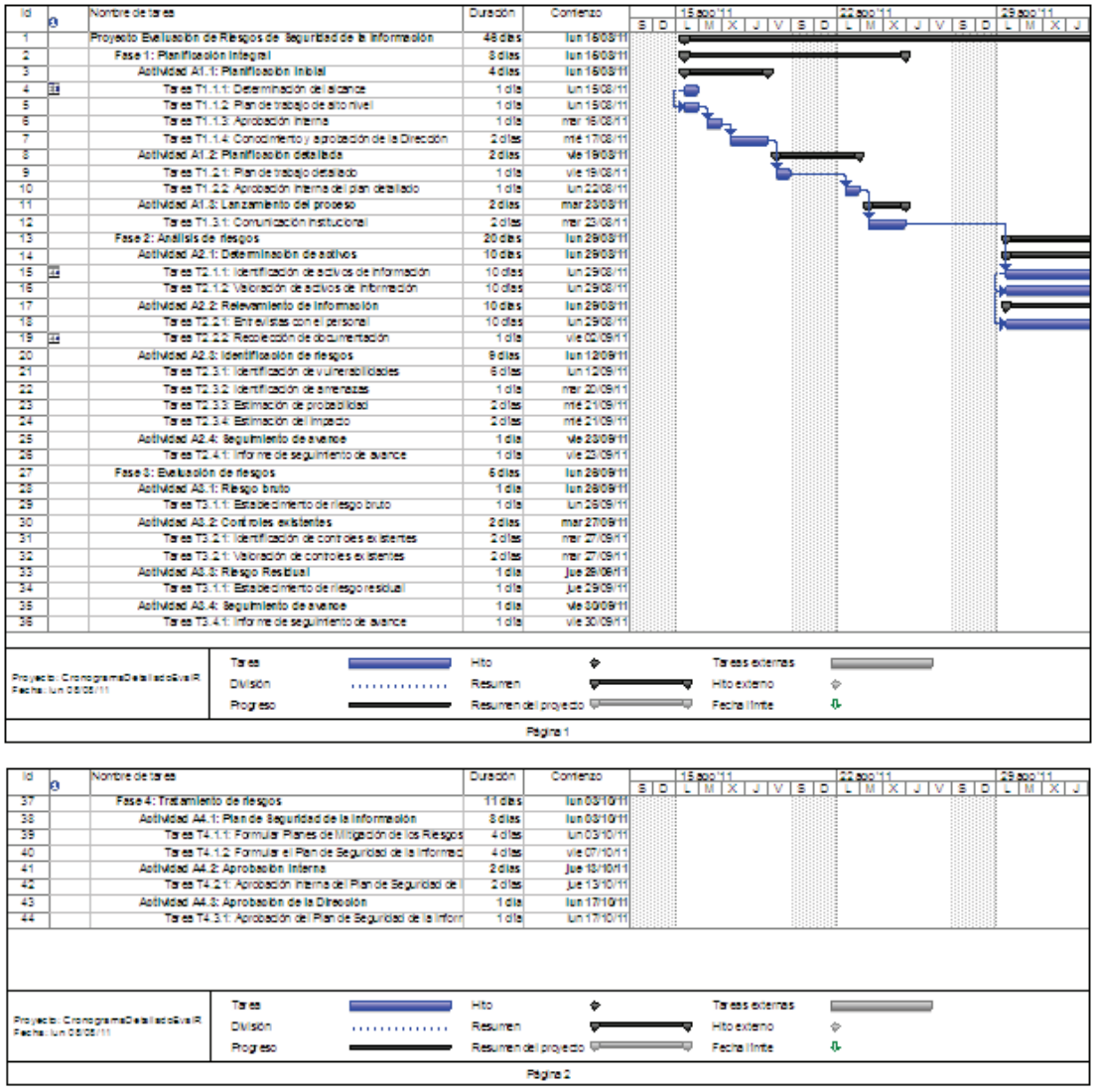
3.3.1.2. Actividad A1.2: Planificación detallada

Los detalles de esta actividad se encuentran en la sección 2.3.3.2

3.3.1.2.1. Tarea T1.2.1: Plan de trabajo detallado

El Departamento Nacional de Seguridad Informática, elabora el siguiente cronograma de trabajo borrador:

Figura No 3.1: Cronograma de trabajo



Elaborado por: *Tania Guevara H.*

3.3.1.2.2. Tarea T1.2.2: Aprobación interna del plan detallado

Tabla No 3.4: Acta de Reunión, aprobación interna del plan detallado

Acta de Reunión

Fecha: Lunes, 22 de Agosto del 2011

Participantes

Xxxxx Xxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxx	Jefe Nacional de Seguridad Informática

Asunto: Presentación y aprobación del cronograma del Proyecto Evaluación de Riesgos de Seguridad de la Información

Temas tratados

- Presentación del cronograma detallado por parte del Jefe de Seguridad Informática - revisión y depuración de tiempos
- La Gerencia Nacional de Riesgos, ratifica y aprueba el cronograma presentado; designa al Jefe de Seguridad Informática como responsable del proyecto, adicional, dos Analistas de Seguridad para trabajar en el mismo; y define que el equipo de trabajo dedicará medio tiempo, en caso de ser necesario, se redefinirá la asignación tanto de tiempo como de recursos.

Resultados – anexos

n/a.

Firma de los participantes

Xxxxx Xxxxxx Gerente Nacional de Riesgos	Xxxxx Xxxxxx Jefe Nal. de Seguridad Informática

Elaborado por: *Tania Guevara H.*

3.3.1.3. Actividad A1.3: Lanzamiento del proceso

3.3.1.3.1. Tarea T1.3.1: Comunicación institucional

La ejecución de esta tarea se realiza mediante el despacho del memorando SI-XXXX2, descrito a continuación (ver sección 2.3.3.3):

MEMORANDO

SI – XXXX2

PARA: Lista adjunta

CC: Xxxxx Xxxxxxx
Subgerente General

DE: Xxxxx Xxxxxxx
Gerente General

ASUNTO: Proyecto Evaluación de Riesgos de Seguridad de la Información

FECHA: Quito, 22 de Agosto del 2011

Como parte del cumplimiento de la Planificación Estratégica de Seguridad Tecnológica, la CFN tiene el importante reto de efectuar una **EVALUACIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACION**, para lo cual, me permito invitar a ustedes a los talleres de relevamiento de información que viabilizará la ejecución de este importante proyecto Institucional.

El objetivo del proyecto es conocer de manera objetiva el estado de la seguridad, determinar la valoración del riesgo de la información Institucional, tomar las medidas de protección apropiadas para los procesos críticos del negocio y panificar su ejecución.

Los talleres se realizarán conforme el cronograma adjunto, para lo cual comprometo su puntual asistencia y el cumplimiento de la agenda planificada, cabe mencionar que es una invitación indelegable e impostergable.

Atentamente,

Xxxxx Xxxxxxx
Gerente General

Anexos: Lo indicado
c.c. Archivo General

Tabla No 3.5: Cronograma de talleres

Fecha	Agenda Reuniones	Hora Inicio	Hora fin
Lunes, 29-ago-11	Xxxxx Xxxxxxx Gerente de División de Fomento y Crédito	09:00	10:00
Lunes, 29-ago-11	Xxxxx Xxxxxxx Gerente de División de Comercio Exterior	10:00	12:00
Lunes, 29-ago-11	Xxxxx Xxxxxxx Gerente Nacional de Concesión de Crédito	12:00	14:00
Martes, 30-ago-11	Xxxxx Xxxxxxx Subgerente Nacional de Crédito de Primer Piso	09:00	12:00
Martes, 30-ago-11	Xxxxx Xxxxxxx Subgerente Nacional de Crédito de Segundo Piso	12:00	14:00
Miércoles, 31-ago-11	Xxxxx Xxxxxxx Subgerente Nal. de Transporte y Prog. Especiales	09:00	11:00
Miércoles, 31-ago-11	Xxxxx Xxxxxxx Subgerente Nac. De Recursos Humanos y DO	11:00	13:00
Jueves, 1-sep-11	Xxxxx Xxxxxxx Gerente Nacional de Coord. de Oficinas y Ventanillas	09:00	10:00
Jueves, 1-sep-11	Xxxxx Xxxxxxx Auditor Interno	10:00	12:00
Jueves, 1-sep-11	Xxxxx Xxxxxxx Subgerente Nacional de Auditoria Informática	12:00	14:00

Lunes, 5-sep-11	Xxxxx Xxxxxxx Gerente de División de Informática	09:00	11:00
Lunes, 5-sep-11	Xxxxx Xxxxxxx Subgerente Nacional de Atención al Usuario	11:00	13:00
Martes, 6-sep-11	Xxxxx Xxxxxxx Subgerente Nacional de Implementación de Sistemas	09:00	14:00
Miércoles, 7-sep-11	Xxxxx Xxxxxxx Subgerente Nacional de Producción y Control	09:00	11:00
Miércoles, 7-sep-11	Xxxxx Xxxxxxx Subgerente Nacional de Infraestructura de TI	11:00	13:00
Jueves, 8-sep-11	Xxxxx Xxxxxxx Gerencia Sucursal Mayor	09:00	12:00
Jueves, 8-sep-11	Xxxxx Xxxxxxx Subgerente Regional de Informática	12:00	17:00
Viernes, 9-sep-11	Xxxxx Xxxxxxx Gerente de Sucursal Ambato	09:00	16:00

Elaborado por: *Tania Guevara H.*

3.3.2. FASE 2: ANÁLISIS DE RIESGOS

3.3.2.1. Actividad A2.1: Determinación de activos

3.3.2.1.1. Tarea T2.1.1: Identificación de activos de información

3.3.2.1.2. Tarea T2.1.2: Valoración de activos de información

Los activos de información se identifican y definen en base al listado de registros y procedimientos vigentes del Sistema de Calidad de la Corporación Financiera Nacional, y se complementa con el inventario de activos existente; su valoración se realiza mediante reuniones de trabajo con los propietarios de la información, quienes evalúan y califican los activos de acuerdo a los siguientes criterios de confidencialidad, integridad y disponibilidad[33]:

Tabla No 3.6: Criterios de confidencialidad

Confidencialidad	
3-Alta	Información que no puede ser divulgada, es de conocimiento limitado a las personas del manejo de la misma, considerada como reservada o confidencial
2-Media	Información que puede ser conocida y utilizada por los funcionarios de la Corporación al interior de la misma
1-Baja	Información de tipo pública, disponible para todos en general

Elaborado por: *Tania Guevara H.*

Tabla No 3.7: Criterios de integridad

Integridad	
3-Alta	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas o graves para la Corporación o terceros

[33] Identificación y valoración de activos aplicando el Procedimiento para Clasificación de la Información (SI-26) y la Norma de Seguridad de la Información relacionada con la Gestión de Activos.

2-Media	Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la CFN, el Sector Público Nacional o terceros
1-Baja	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad de la CFN

Elaborado por: *Tania Guevara H.*

Tabla No 3.8: Criterios de disponibilidad

Disponibilidad	
3-Alta	Información cuya inaccesibilidad durante 4 horas podría ocasionar pérdidas significativas o graves a la Corporación o a terceros
2-Media	Información cuya inaccesibilidad durante 1 día podría ocasionar pérdidas materiales, de imagen, de valor estratégico de la información, de obligaciones contractuales o públicas, de disposiciones legales, etc. significativas para la Corporación o terceros
1-Baja	Información cuya inaccesibilidad no afecta la operatividad

Elaborado por: *Tania Guevara H.*

Tabla No 3.9: Tipo de Información (grado de sensitividad)

Tipo de Información (grado de sensitividad)	
Reservada Confidencial	Criticidad Alta: alguno de los valores asignados es 3
De uso Interno	Criticidad Media: alguno de los valores asignados es 2
Pública	Criticidad baja: ninguno de los valores asignados superan el 1

Elaborado por: *Tania Guevara H.*

El objetivo y por menores de estas tareas se describen en la sección 2.3.4.1

El resultado en detalle del inventario de activos valorados se anexa en el documento "ClasificacionInformacionFinal.xls"; a continuación se muestra un extracto del "Listado Índice temático de Información Reservada" y "Clasificación de la Información por el Grado de Sensitividad".

Tabla No 3.10: Listado índice temático de información reservada

LISTADO INDICE TEMATICO DE INFORMACION RESERVADA					
INFORMACION CONFIDENCIAL / RESERVADA					
Índice	**ACTIVO DE INFORMACION**	**IDENTIFICACION**	**Custodia**	**Breve detalle del Contenido**	**Responsable**
1	Expedientes sobre clientes de productos y servicios de la CFN	Información generada en operaciones de la CFN: Clientes y operaciones de Crédito, Fiducia, IFI's, Participación Accionaria, Comercio Exterior y demás productos y servicios generados en todos los procesos de la CFN	Archivo General	Información de Clientes	Áreas del proceso
2	Expedientes por Control de Lavado de Activos, Atención a Clientes y Seguridad Informática	Documentos, información y anexos por las actividades de Control de Lavado de Activos, Atención a Clientes y Seguridad Informática	Áreas de los procesos	Información clientes / Institucional	Coord. Org. Control
3	Expedientes de Directorio	Convocatorias, actas, informes y reportes internos, resoluciones de sesiones de directorio	Secretaria General	Información Institucional	Secretaria General

Elaborado por: *Tania Guevara H.*

Tabla No 3.11: Información de uso interno

CLASIFICACIÓN DE LA INFORMACIÓN POR EL GRADO DE SENSITIVIDAD						
INFORMACION DE USO INTERNO						
Código del Activo de Información	**Activo de Información**	**Código del Procedimiento**	**Procedimiento**	**Custodia del activo**	**Breve detalle del Contenido de la información**	**Área Responsable**
RPCP-02	Registro de entrega de carpeta cliente a archivo	PCP-02 PCP-03	…..Procedimiento para instrumentar operaciones y ejecutar desembolsos	Archivo General	Información crédito	Crédito 1Piso

RPCP-23	Formulario de atención al cliente	PCP-01	Procedimiento para precalificar solicitudes de crédito	Archivo General	Información cliente	Crédito 1Piso
RPCR-01	Registro de documentos entregados a Finanzas	PCR-01	Procedimiento para colocar crédito	Crédito 2Piso	Información Crédito	Crédito 2Piso
RPCR-03	Reg. de dctos. entregados al archivo	PCR-01	Procedimiento para colocar crédito	Crédito 2Piso	Información general	Crédito 2Piso

Elaborado por: *Tania Guevara H.*

Tabla No 3.12: Información pública

CLASIFICACIÓN DE LA INFORMACIÓN POR EL GRADO DE SENSITIVIDAD						
INFORMACION PUBLICA						
Código del Activo de Información	**Activo de Información**	**Código del Procedimiento**	**Procedimiento**	**Custodia del activo**	**Breve detalle del Contenido de la información**	**Área Responsable**
RPCR-16	Registro de revisión del contrato	PCR-01	Procedimiento para colocar crédito	Archivo General	Información Crédito	Crédito 2Piso
	Cartas y documentos de promoción crédito asociativo			Microcrédito	Promoción línea de crédito asociativo	Microcrédito

Elaborado por: *Tania Guevara H.*

3.3.2.2. Actividad A2.2: Relevamiento de información

3.3.2.2.1. Tarea T2.2.1: Entrevistas con el personal

Las reuniones para relevamiento de información se llevan a cabo conforme calendarización adjunta en memorando SI-XXXX2, la información proporcionada por el entrevistado se recoge en el formulario “Registro de Levantamiento de Información” (Anexo A) y se suscribe un acta de reunión que evidencia el cumplimiento de esta tarea (ver sección 2.3.4.2, tarea T2.2.1).

A manera de ejemplo se describe a continuación el relevamiento realizado en la Subgerencia Nacional de Crédito de Primer Piso.

Tabla No 3.13: Acta de Reunión, entrevista

Acta de Reunión

Fecha: Martes, 30 de Agosto del 2011

Participantes

Xxxxx Xxxxxxx	Subgerente Nacional de Crédito de Primer Piso
Xxxxx Xxxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxxx	Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática

Asunto: Relevamiento de información del proyecto de evaluación de riesgos de seguridad de la información

Temas tratados

- Presentación de objetivos del proyecto
- Descripción general de los procesos y productos de Primer Piso
- Encuesta sobre temas puntales de seguridad de la información
- Expectativas de seguridad de la información de Primer Piso

Resultados

Registro de Levantamiento de Información tomado por personal del Área de Seguridad Informática.

Firma de los participantes

Xxxxx Xxxxxxx Subgerente Nal Crédito Primer Piso	Xxxxx Xxxxxxx Gerente Nacional de Riesgos
Xxxxx Xxxxxxx Jefe Nal. de Seguridad Informática	Xxxxx Xxxxxxx Analista de Seguridad Informática

Xxxxx Xxxxxxx Analista de Seguridad Informática	

Elaborado por: *Tania Guevara H.*

Tabla No 3.14: Registro de Levantamiento de Información

CONFIDENCIAL	
Registro de Levantamiento de Información **Gestión de Riesgos de Seguridad de la Información**	
Fecha:	30 de agosto del 2011
1. Datos personales	
Nombre:	Xxxxx Xxxxxxx
Cargo:	Subgerente Nacional de Crédito de Primer Piso
Área:	Subgerencia Nacional de Crédito de Primer Piso
2. Relevamiento de Información	
2.1 Descripción general del proceso, área o producto	
Área de negocios, modelo de gestión basado en procesos, crédito directo (mayor valor para la entidad, por su volumen que representa dentro de la institución). Proceso de concesión de crédito: Comienza con la precalificación, que es la entrega de información a los clientes, son créditos productivos, se valida la central de riesgos y que cumpla con ciertas políticas de crédito sobre actividades financiables como son productivas, comerciales; en un plazo máximo de 30 días el cliente debe entregar la documentación, esto lo hacen los oficiales de precalificación, que tiene una jefatura, existen 6 analistas. Luego de entregada la documentación se hace una breve validación de que la información este completa, se genera una solicitud de crédito en el sistema COBIS, con aprobación de la jefatura, ese expediente se asigna a un oficial de crédito y pasa a la etapa de análisis, quien revisa la información y el oficial de crédito se contacta con el cliente, el oficial solicita que se haga un avalúo de las	

garantías, y se acuerda una visita de la empresa in situ (próximos 7-8 días), en la visita a la empresa se detalla información financiera, aclaración de información, se afina la información enviada por el cliente.

Luego de la visita a la empresa, se hace un informe de crédito, lo revisa el jefe y se somete a una instancia de aprobación, en esta instancia intervienen los comités de crédito dependiendo del monto, el comité emite la aprobación del crédito y se le da a conocer al cliente los términos en que se aprobó el crédito y luego pasa a la siguiente etapa de 90 días que es la instrumentación, el cliente debe complementar información solicitada y podría aplazarse 90 días más, se ingresa las condiciones financieras de la operación y se registra en el sistema COBIS. Esta fase es la más delicada, y debe validarse que la información completa se ingrese correctamente al sistema.

Luego se coordina con el departamento legal la fecha para la suscripción del contrato de crédito, y pasa inmediatamente al desembolso, con el primer desembolso concluye con el proceso de crédito.

Productos:

Crédito directo (destinos: activos fijos: maquinaria y equipos, capital de trabajo: materia prima, insumos – corto plazo, línea revolvente de capital de trabajo: mano de obra, insumos, materia prima – se firma una sola vez como tarjeta de crédito con cupo - sobregiro)

2.2 Aspectos relevantes de Seguridad de la Información

2.2.1. Política de Seguridad

Tema de claves para acceso a los sistemas son personales e intransferibles, manejo con sigilo.

Vacaciones o ausencia, con anticipación se coordina e informa para asignar los roles temporales (dos días antes) – no sabe con exactitud dónde está escrito.

Buena práctica de escritorios limpios en ausencias largas (únicamente en la noche)

2.2.2. Aspectos Organizativos de la Seguridad de la Información

n/a

2.2.3. Gestión de Activos

n/a

2.2.4. Seguridad Ligada a los Recursos Humanos

La gente está consciente en manejo de información sensible, no comparte

claves. Información sensible: Información del cliente desde la información financiera, patrimonial y garantías, composición accionaria de las empresas, informes de avalúos, los proyectos de los clientes, documentos valorados. Información básica del cliente es menos confidencial (nombres, dirección). Los computadores se bloquean automáticamente, sin embargo, el usuario no bloquea por sí mismo.
2.2.5. Seguridad Física y Ambiental n/a
2.2.6. Gestión de Comunicaciones y Operaciones Virus, no han tenido Cuantas veces se va el sistema: 1 vez al mes, por 1 hora en promedio, máximo 4 horas. Los sistemas son ágiles en matriz a toda hora, en regionales es lento incluso el correo electrónico Auditoria: Con ayuda de informática, cambio de estados de la operación de crédito, se requiere conocer quien autorizó – cambió dicho estado. Los usuarios ven cierto tipo de rastros: usuario, fecha, estado de la operación pero no en todas las operaciones No hay alertas en los sistemas.
2.2.7. Control de Accesos Identificación: Red: 1 usr, Notes: 1 usr, Cobis: 1 usr, PCIE riesgos: 1 usr, PCIE servicios al funcionario: 1 usr Claves: 3 Perfiles de acceso: define en el área (propietario) se revisa cada 6 meses; RRHH si hay un nuevo cargo el jefe define las funciones, e informa a seguridad informática para coordinar con la jefatura los roles. Cuando se van de vacaciones se agregan los roles al backup pero el sistema controla los niveles de autorización, para ver información, podría ver lo de los dos cargos.

Personal nuevo, hay formulario para pedir claves, subgerente de área y RRHH. Vacaciones, por correo electrónico. Cambios administrativos, por formulario, subgerente de área y RRHH. Salidas, por memo de RRHH.
2.2.8. Adquisición, mantenimiento y desarrollo de los sistemas de información n/a
2.2.9. Gestión de Incidentes de Seguridad n/a
2.2.10. Gestión de Continuidad del negocio n/a
2.2.11. Cumplimiento n/a
2.3. Expectativas / Sugerencias
Que exista una única cara al cliente. Con BPM piensa que se cubrirá riesgos operativos (no se van a saltar procesos, se digitalizan documentos, hay control de tiempos) Mayor conciencia de uso de claves para que no compartan, con talleres o boletines a niveles gerencial

Elaborado por: *Tania Guevara H.*

3.3.2.2.2. Tarea T2.2.2: Recolección de documentación

Con la finalidad de contar con elementos que sirvan de fuente de información adicional para corroborar, aclarar y/o complementar la información proporcionada por los funcionarios entrevistados en la tarea T2.2.1, se recopila políticas de Tecnología de la Información, Seguridad de la Información, normas, procedimientos e instructivos tanto operativos como técnicos; Plan Estratégico Institucional y de Tecnología, Plan de Recuperación de Desastres y Continuidad del Negocio, entre otros (ver sección 2.3.4.2, tarea T2.2.2).

3.3.2.3. Actividad A2.3: Identificación de riesgos

3.3.2.3.1. Tarea T2.3.1: Identificación de vulnerabilidades

Luego de haber entrevistado al personal idóneo en el proceso de relevamiento de información y contar con documentación adicional que ayude a comprender los planes, normativa y procesos institucionales, se unifica toda la información proporcionada por los entrevistados, sobre esta base se identifican hechos positivos y negativos, los mismos que están relacionados y clasificados en los diferentes aspectos relevantes de seguridad de la información.

Los hechos negativos se consideran como fallas o insuficiencias propias de la CFN (vulnerabilidades) que pueden afectar a la seguridad de la información; y, los hechos positivos constituyen oportunidades de mejora para la gestión de seguridad de la información.

El listado de vulnerabilidades detectadas fruto del relevamiento de información se muestra en una matriz de riesgos al finalizar la tarea T3.1.1: Establecimiento de riesgo bruto de la fase 3: Evaluación de Riesgos; la matriz detalla todos los elementos relacionados con vulnerabilidades, amenazas, probabilidad, impacto y riesgo bruto. Esta actividad está descrita en la sección 2.3.4.3, tarea T2.3.1.

3.3.2.3.2. Tarea T2.3.2: Identificación de amenazas

A cada vulnerabilidad detectada en la tarea anterior se debe prestar atención únicamente si existe alguna amenaza que pueda aprovechar dicho hueco de seguridad y derivar en un incidente, bajo esta premisa, para cada vulnerabilidad se identifica y asocia una o más amenazas, con la ayuda del catálogo de amenazas (anexo B).

Para oportunidades de mejora no es aplicable la identificación y asociación de amenazas, por consiguiente, para este tipo de hallazgos no se estima probabilidad, impacto, riesgos ni controles (ver sección 2.3.4.3, tarea T2.3.2).

El detalle de las amenazas identificadas se detalla al finalizar la tarea T3.1.1: Establecimiento de riesgo bruto de la fase 3: Evaluación de Riesgos.

3.3.2.3.3. Tarea T2.3.3: Estimación de probabilidad

En base al Anexo C – Criterios para Calificar la Probabilidad de Ocurrencia, se establece la posibilidad de que la(s) amenaza(s) identificada(s) en la tarea T2.3.2 puedan explotar su vulnerabilidad asociada. La probabilidad de ocurrencia se define tomando en cuenta el valor de los activos de información y considerando las respuestas obtenidas en el proceso de entrevistas, las mismas que en su mayoría son fruto de la experiencia (historia) propia de los funcionarios entrevistados (ver sección 2.3.4.3, tarea T2.3.3).

Para facilitar la ejecución de esta tarea, por cada amenaza/vulnerabilidad se debe preguntar: ¿Cuán frecuente es o sería, que se materialice la amenaza, debido a que existe la vulnerabilidad?

La determinación de la probabilidad se muestra al finalizar la tarea T3.1.1: Establecimiento de riesgo bruto de la fase 3: Evaluación de Riesgos

3.3.2.3.4. Tarea T2.3.4: Estimación del impacto

Se pondera el nivel de impacto que causaría si llegara a materializarse la(s) amenaza(s) debido a que existe una vulnerabilidad; de forma similar que en la tarea anterior, para la determinación del impacto se basa en la definición del Anexo D – Criterios para Calificar el Nivel de Impacto, se considera la importancia de los activos y la información proporcionada por los entrevistados (ver sección 2.3.4.3, tarea T2.3.4).

La ejecución de esta tarea se facilita con la siguiente pregunta: ¿Qué pasaría si, se efectiviza la amenaza, debido a que existe la vulnerabilidad?

Los resultados en detalle de la determinación del impacto se listan al finalizar la tarea T3.1.1: Establecimiento de riesgo bruto de la fase 3: Evaluación de Riesgos

3.3.2.4. Actividad A2.4: Seguimiento de avance

3.3.2.4.1. Tarea T2.4.1: Informe de seguimiento de avance

Tabla No 3.15: Acta de Reunión, análisis de riesgos, informe seguimiento

Acta de Reunión

Fecha: Viernes, 23 de Septiembre del 2011

Participantes

Xxxxx Xxxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxxx	Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática

Asunto: Seguimiento de avance del proyecto de evaluación de riesgos de seguridad de la información

Temas tratados

- Se revisa el cumplimiento de las actividades detalladas en el cronograma de trabajo del proyecto
- Se analiza el avance de las actividades hasta la fase 2
- Se valida que no ha existido dificultades en el cumplimiento del cronograma
- A continuación se detalla cada tarea con el resumen de lo realizado:

Avance del Proyecto Evaluación de Riesgos de Seguridad de la Información

Fase / Actividad / Tarea	**Avance**
Fase 2 – Análisis de Riesgos / Actividad A2.1: Determinación de activos	
Tarea T2.1.1: Identificación de activos de información Tarea T2.1.2: Valoración de activos de información	100% completado, levantamiento de los activos por parte del equipo de trabajo, calificación de los activos por parte de los propietarios de la información.
Fase 2 – Análisis de Riesgos / Actividad A2.2: Relevamiento de información	
Tarea T2.2.1: Entrevistas con el personal	100% completado, reuniones de trabajo con los propietarios de información y funcionarios designados, levantamiento de información por funcionarios de Seguridad Informática.
Tarea T2.2.2: Recolección de documentación	100% completado, para la recolección de información adicional se tiene como fuentes a la Intranet y Sistema de Calidad de la CFN.
Fase 2 – Análisis de Riesgos / Actividad A2.3: Identificación de riesgos	
Tarea T2.3.1: Identificación de vulnerabilidades Tarea T2.3.2: Identificación de amenazas	100% completado, el listado de vulnerabilidades con sus respectivas amenazas se encuentran en la Matriz de Riesgos.
Tarea T2.3.3: Estimación de probabilidad Tarea T2.3.4: Estimación del impacto	100% completado, la probabilidad e impacto ponderados se detallan en la Matriz de Riesgos, las estimaciones se establecieron en base a los criterios definidos para calificar probabilidad de ocurrencia y nivel de impacto.

- La fase 2 está concluida al 100%.

Resultados

Cronograma de trabajo actualizado con el porcentaje de avance del proyecto.

Firma de los participantes

Xxxxx Xxxxxxx Gerente Nacional de Riesgos	Xxxxx Xxxxxxx Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx Analista de Seguridad Informática	Xxxxx Xxxxxxx Analista de Seguridad Informática

Elaborado por: *Tania Guevara H.*

3.3.3. FASE 3: EVALUACIÓN DE RIESGOS

3.3.3.1. Actividad A3.1: Riesgo bruto

3.3.3.1.1. Tarea T3.1.1: Establecimiento de riesgo bruto

Considerando que el riesgo bruto constituye la totalidad del riesgo sin tomar en cuenta los controles o salvaguardas existentes, se establece el nivel de riesgo bruto combinando probabilidad de ocurrencia e impacto conforme lo establecido en el Anexo E – Criterios para calificar el riesgo bruto (ver sección 2.3.5.1, tarea T3.1.1).

A continuación se ejemplifica la forma de presentar los resultados de la metodología de evaluación de riesgos de seguridad de la información aplicada hasta el momento.

Tabla No 3.16: Matriz de Riesgos Brutos

Matriz de Riesgos Brutos Corporación Financiera Nacional						
Dominio	**No**	**Amenaza**	**Vulnerabilidad / Oportunidad de Mejora**	**Probabilidad**	**Impacto**	**Riesgo Bruto**
Política Seguridad	1	No aplica	Existe una política y tres normas de seguridad de la información institucional basada en la norma ISO/IEC 27001, las mismas que son revisadas periódicamente conforme una planificación. La política tiene definido sanciones por incumplimiento, al momento solo se ha sido necesario hacer llamados de atención. La mayoría de funcionarios conocen de la política la parte que les corresponde aplicar, sin embargo, sería importante hacer mayor difusión de la misma. Algunos funcionarios consideran que ponen en práctica ciertos aspectos de seguridad por cuenta propia, por ejemplo, escritorios limpios, dado que aprendieron en otras instituciones; consideran que este tema no forma parte de la política. (Oportunidad de Mejora)	No aplica	No aplica	No aplica
	2	Genera incidentes de seguridad	Existen normas, estándares y procedimientos (operativos y técnicos) de seguridad, sin embargo, la documentación no es completa, faltaría documentar aspectos relacionados a evaluación de riesgos, gestión de incidentes de seguridad, etc. De igual forma, incluir seguridad en procedimientos relacionados, tales como, control y gestión de tecnología, por ejemplo, programación segura.	Alta	Mayor	Superior
Seguridad RRHH	3	Genera incidentes de seguridad	El proceso de selección de personal, no incluye una evaluación formal relacionada a investigación del aspirante (antecedentes). Algunos pasantes van a puestos críticos y no siguen el mismo procedimiento de selección, y no reciben inducción institucional.	Moderada	Mayor	Superior
	4	Indisponibilidad del personal	En algunas áreas se ha definido personal alterno que cuando está operando causa que no haya división de funciones, esto por falta de recursos, por ejemplo en tecnología y sucursales	Alta	Mayor	Superior
	5	Genera incidentes de seguridad	Existe un programa de concienciación de seguridad de la información formal. Se ha dado capacitación en materia de seguridad, sin embargo, es importante validar que dicha capacitación haya llegado a todos los funcionarios	Baja	Mayor	Alto
	6	Genera incidentes de seguridad	Existe conciencia que no se puede prestar el usuario/clave, pero se presentan casos en que se comparten claves por enfermedad, vacaciones, para soporte técnico. En el caso de mantenimiento de proveedores se presta el acceso (el funcionario escribe su clave, pero trabaja el proveedor). Algunos, luego de estos casos eventuales piden a seguridad cambio de clave.	Moderada	Mayor	Superior
	7	Suplantación de identidad; Pérdida de inf.	Los funcionarios no bloquean sus PC's al abandonar su puesto de trabajo porque se bloquea automáticamente luego de un tiempo, adicionalmente, no dejan guardada documentación física sensible	Moderada	Mayor	Superior

Gestión de Comunicaciones y Operaciones	8	Acceso no autorizado	Se maneja una red plana, sin segmentación de ningún tipo	Moderada	Mayor	Superior
	9	Intercepción de información	La red de datos no tiene protección (cifrado) para el tránsito de información confidencial, de la misma forma información confidencial transmitida por correo electrónico no es cifrada.	Baja	Mayor	Alto
	10	Acceso no autorizado	Está permitido hacer administración remota de servidores vía VNC desde cualquier PC de la red, en algunos casos está configurado sin clave a pesar que los servidores siempre están bloqueados localmente.	Moderada	Mayor	Superior
	11	Difusión de software dañino	Se encuentran desactualizadas los parches de las PC's, este proceso no se lo está ejecutando, no se cuenta con un laboratorio para validaciones previas.	Alta	Moderado	Alto
	12	Fuga de información; Manipulación de la configuración	Existe información crítica en los Pc's sin encriptar, por ejemplo, el personal alterno técnico cuando entra en funciones registra en un archivo (sin encripción) las contraseñas de administración de BD, a pesar de tener contraseña de acceso, el archivo no está encriptado.	Moderada	Mayor	Superior
	13	Pérdida de información	Para respaldo de información en estaciones de trabajo se ha implementado la herramienta iFolder, que su respaldo es manual, otras áreas (no del negocio) respaldan su información en discos externos. (Pasar a comunicaciones)	Baja	Moderado	Moderado
	14	Denegación de servicio	La administración de base de datos no tiene una normativa definida en relación a la planificación de capacidad y rendimiento, esta actividad se la realiza conforme se presentan los requerimientos.	Moderada	Mayor	Superior
	15	Denegación de servicio	Los cortes de servicios informáticos prolongados en horarios laborales son eventuales (3 al año aproximado), sin embargo, por cierre de sistemas (cierre contable) no se cuenta con el servicio del sistema COBIS estable por dos días a fin de mes y se pierde tiempo de trabajo de los funcionarios de negocio. No hay Acuerdos de Niveles de Servicio definidos.	Muy Alta	Mayor	Superior
	16	Fraude	Falta desarrollar procedimientos para revisiones periódicas de pistas de auditoria, log's de seguridad y acciones de usuarios privilegiados.	Moderada	Mayor	Superior
	17	Genera incidentes de seguridad	Debido a que la auditoria está implementada en el aplicativo, las pistas de auditoria no guardan la misma información para los eventos auditados, en otros casos no se audita el evento y en la mayoría no existe un reporte desde el aplicativo para ver dicha información.	Alta	Mayor	Superior
	18	Acceso no autorizado; Fuga y alteración de información	Se hace monitoreo de usuarios funcionales sobre las acciones de seguridad (uso adecuado de recursos, uso de claves, intentos fallidos, etc.), debe también aplicarse el monitoreo a usuarios privilegiados como administradores de BD, cambios de parametrizaciones contables, acciones de proveedores en ambientes de producción.	Baja	Mayor	Alto

	19	Genera incidentes de seguridad; Manipulación de programas	Se maneja auditoría a nivel de base de datos solo para el usuario "sa", para los aplicativos de negocio la auditoria se programa en el propio aplicativo por lo que depende del técnico la implementación de la misma, situación que no refleja confiabilidad en los rastros obtenidos sea por error en la programación o porque no se la consideró incompleta o no se la consideró. No hay auditoria para consultas.	Alta	Mayor	Superior
	20	Genera incidentes de seguridad	Los aplicativos de negocio no tienen implementados las facilidades de alertas tempranas, es importante que se implementen alertas relacionadas al negocio como de seguridad.	Moderada	Mayor	Superior
	21	Denegación de servicio	Sólo algunos de los equipos tecnológicos tienen implementadas alertas tempranas (red, servidores - Inside Manager o Virtual Center vía correo. Las BD no tienen alertas.	Moderada	Mayor	Superior
Control Accesos	22	Errores de usuario	La CFN tiene implementadas herramientas de Secure Login, Identity Manager y Novell (eDirectory) para manejar identificación y autenticación, sin embargo, la solución de seguridad no está integrada a todos los sistemas (Gestor-fiducia, Risk Control Services y Qlik View).	Moderada	Menor	Moderado
	23	Suplantación de identidad; Fuga de información	La estructura de la contraseña (autenticación) no es estándar en todas las aplicaciones y sw (PCIE's no acepta caracteres especiales y es case-insensitive, COBIS no acepta caracteres especiales y es case-sensitive, Intranet acepta caracteres especiales y es case-sensitive, en algunas Pc's la clave del administrador esta en blanco.	Moderada	Moderado	Alto
	24	Suplantación de identidad; Fuga de información; Fraude	Las características de la contraseña (autenticación) no son estándar y en algunos casos no son seguras, por ejemplo: Red y PCIE's v5 y 9 expira cada 30 días, v6 no expira, COBIS cada 60. Sólo la Red pide cambio de clave la primera vez o cuando el administrador resetea la misma. Sólo la Red y COBIS registra intentos fallidos y controlan contraseñas históricas. La Red, COBIS y PCIE's controlan el número de instancias. PCIE's no bloquean la cuenta luego de intentos fallidos de acceso. La Red y COBIS tienen administración de horarios.	Moderada	Moderado	Alto
	25	Suplantación de identidad; Fuga de información	Los mecanismos de autenticación están implementados dentro de los sistemas, es decir, los usuarios, claves y privilegios residen en tablas de BD. COBIS maneja 3DES. PCIE's registra contraseña plana (nadie tiene acceso a esta tabla sólo el adm de BD. El login de BD de PCIE's está encriptado.	Moderada	Moderado	Alto
	26	Acceso no autorizado; Indisponibilidad de personal	Claves sensibles como la del administrador de BD, de servidores, elementos de comunicaciones son manejadas por una sola persona. Falta elaborar un procedimiento para manejo de claves sensibles.	Alta	Mayor	Superior
	27	Acceso no autorizado	Es posible administrar los servidores desde cualquier PC, incluso desde sucursales. Se ha dado acceso remoto a proveedores de forma controlada. El soporte a usuarios se ejecuta mediante acceso remoto a las PC's que tiene la posibilidad de no solicitar aprobación al dueño del equipo.	Moderada	Mayor	Superior

	28	Manipulación de la configuración; Fuga y alteración de información	Los servicios de seguridad perimetral están tercerizados por lo que debe existir acuerdos claros y documentados para de poder auditar y monitorear las acciones del proveedor	Baja	Mayor	Alto
	29	Genera incidentes de seguridad	El área de auditoria informática no realiza pruebas de ethical hacking ni auditoria forense puesto que no está definido entre sus funciones. Se ha realizado un prueba de ethical hacking liderado por el área de Seguridad Informática	Moderada	Mayor	Superior
	30	Fuga de información	El sistema Informes Cobis es de reportería que tiene claves genéricas, se puede bajar a Excel y es utilizada por varias áreas como cartera, prevención de lavado de activos, planeación, etc. El personal de desarrollo usa ISQL para consultar data de producción. Para ambos casos no queda registro de la actividad del usuario	Moderada	Mayor	Superior
	31	Acceso no autorizado	Los cambios de roles por cambios administrativos son manuales por lo que a veces ciertos funcionarios se quedan con los privilegios de ambas funciones (anterior y nueva).	Baja	Mayor	Alto
	32	Acceso no autorizado	La administración total de los equipos tecnológicos está a cargo de la Gerencia de División de Informática, por lo que usuarios en servidores y base de datos creados por funcionarios de esta gerencia.	Moderada	Mayor	Superior

Elaborado por: *Tania Guevara H.*

3.3.3.2. Actividad A3.2: Controles existentes

3.3.3.2.1. Tarea T3.2.1: Identificación de controles existentes

3.3.3.2.2. Tarea T3.2.2: Valoración de controles existentes

Para un adecuado relevamiento y valoración de controles existentes es necesario identificar a los funcionarios responsables tanto de la ejecución como de la validación del cumplimiento del control, esta tarea se realiza como parte del proceso de entrevistas en donde los principales involucrados son el personal del Área de Informática, Seguridad Informática y Auditoría Interna.

Es importante hacer un levantamiento del control o controles implementados por cada una de las vulnerabilidades detectadas. La calificación de la eficacia de los controles se enriquece con la validación de resultados de auditorías internas, externas, de organismos de control, comité de auditoría, entre otras; adicionalmente se recoge evidencia de aplicación y periodicidad de ejecución de los controles, a fin de tener certeza de su cumplimiento (ver sección 2.3.5.1, tarea T3.1.2).

A continuación se muestra el detalle de la identificación y valoración de controles existentes:

Tabla No 3.17: Lista de controles

Lista de Controles Corporación Financiera Nacional										
Dom	**No**	**Vulnerabilidad / Oportunidad de Mejora**	**Nombre del Control**	**Responsable**	**Tipo**	**Naturaleza**	**Frecuencia**	**Operativo**	**Observado**	**Eficacia**
Política Seguridad	1	Existe una política y tres normas de seguridad de la información institucional basada en la norma ISO/IEC 27001, las mismas que son revisadas periódicamente conforme una planificación. La política tiene definido sanciones por incumplimiento, al momento solo se ha sido necesario hacer llamados de atención. La mayoría de funcionarios conocen de la política la parte que les corresponde aplicar, sin embargo, sería importante hacer mayor difusión de la misma. Algunos funcionarios consideran que ponen en práctica ciertos aspectos de seguridad por cuenta propia, por ejemplo, escritorios limpios, dado que aprendieron en otras instituciones; consideran que este tema no forma parte de la política. (Oportunidad de Mejora)	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica	No aplica
	2	Existen normas, estándares y procedimientos (operativos y técnicos) de seguridad, sin embargo, la documentación no es completa, faltaría documentar aspectos relacionados a evaluación de riesgos, gestión de incidentes de seguridad, etc. De igual forma, incluir seguridad en procedimientos relacionados, tales como, control y gestión de tecnología, por ejemplo, programación segura.	En proceso de implementación programación segura (QA)	Gerencia de División de Informática	Preventivo	Manual	Por demanda	No	No	Débil

Seguridad RRHH	3	El proceso de selección de personal, no incluye una evaluación formal relacionada a investigación del aspirante (antecedentes). Algunos pasantes van a puestos críticos y no siguen el mismo procedimiento de selección, y no reciben inducción institucional.	Pasantes participan en inducciones generales	Subgerencia Nacional de RRHH y DO	Preventivo	Manual	Por demanda	Si	No	Moderado
	4	En algunas áreas se ha definido personal alterno que cuando está operando causa que no haya división de funciones, esto por falta de recursos, por ejemplo en tecnología y sucursales	Control de Jefaturas	Todas las áreas	Detectivo	Manual	Por demanda	Si	No	Débil
	5	Existe un programa de concienciación de seguridad de la información formal. Se ha dado capacitación en materia de seguridad, sin embargo, es importante validar que dicha capacitación haya llegado a todos los funcionarios	Programa de concienciación de seguridad de la información	Seguridad Informática	Preventivo	Manual	Trimestral	Si	No	Moderado
	6	Existe conciencia que no se puede prestar el usuario/clave, pero se presentan casos en que se comparten claves por enfermedad, vacaciones, para soporte técnico. En el caso de mantenimiento de proveedores se presta el acceso (el funcionario escribe su clave, pero trabaja el proveedor). Algunos, luego de estos casos eventuales piden a seguridad cambio de clave.	Revisión de log's; Llamados de atención; Boletines informativos periódicos virtuales; Revisión uso de recursos; Concienciación a empleados; Inducción empleados nuevo; Difusión general de la política	Seguridad Informática	Preventivo	Manual	Trimestral	Si	No	Moderado
	7	Los funcionarios no bloquean sus PC's al abandonar su puesto de trabajo porque se bloquea automáticamente luego de un tiempo, adicionalmente, no dejan guardada documentación física sensible	Bloqueo PC (en 10 min)	Gerencia de División de Informática	Preventivo	Manual	Constante	Si	No	Moderado

Gestión de Comunicaciones y Operaciones	8	Se maneja una red plana, sin segmentación de ningún tipo	Serán implementadas VLAN's	Gerencia de División de Informática	Preventivo	Automático	Constante	No	No	Débil
	9	La red de datos no tiene protección (cifrado) para el tránsito de información confidencial, de la misma forma información confidencial transmitida por correo electrónico no es cifrada.	Por enlaces de datos la Información viaja segura garantizado por el proveedor.	Gerencia de División de Informática	Preventivo	Manual	Constante	Si	No	Moderado
	10	Está permitido hacer administración remota de servidores vía VNC desde cualquier PC de la red, en algunos casos está configurado sin clave a pesar que los servidores siempre están bloqueados localmente.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil
	11	Se encuentran desactualizadas los parches de las PC's, este proceso no se lo está ejecutando, no se cuenta con un laboratorio para validaciones previas.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil
	12	Existe información crítica en los Pc's sin encriptar, por ejemplo, el personal alterno técnico cuando entra en funciones registra en un archivo (sin encripción) las contraseñas de administración de BD, a pesar de tener contraseña de acceso, el archivo no está encriptado.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil
	13	Para respaldo de información en estaciones de trabajo se ha implementado la herramienta iFolder, que su respaldo es manual, otras áreas (no del negocio) respaldan su información en discos externos. (Pasar a comunicaciones)	IFolder; Norma de control de accesos	Gerencia de División de Informática; Seguridad Informática	Preventivo	Manual	Por demanda	No	No	Débil
	14	La administración de base de datos no tiene una normativa definida en relación a la planificación de capacidad y rendimiento, esta actividad se la realiza conforme se presentan los requerimientos.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil

	15	Los cortes de servicios informáticos prolongados en horarios laborales son eventuales (3 al año aproximado), sin embargo, por cierre de sistemas (cierre contable) no se cuenta con el servicio del sistema COBIS estable por dos días a fin de mes y se pierde tiempo de trabajo de los funcionarios de negocio. No hay Acuerdos de Niveles de Servicio definidos.	Está en proceso la actualización de HW y SW de core bancario.	Gerencia de División de Informática	Preventivo	Automático	Constante	No	No	Débil
	16	Falta desarrollar procedimientos para revisiones periódicas de pistas de auditoría, log's de seguridad y acciones de usuarios privilegiados.	Procedimiento de revisión de Log's para bdd y servidores críticos	Seguridad Informática	Detectivo	Manual	Por demanda	Si	Si	Débil
	17	Debido a que la auditoria está implementada en el aplicativo, las pistas de auditoria no guardan la misma información para los eventos auditados, en otros casos no se audita el evento y en la mayoría no existe un reporte desde el aplicativo para ver dicha información.	Política y Norma de seguridad	Todas las áreas	Detectivo	Manual	Constante	No	Si	Débil
	18	Se hace monitoreo de usuarios funcionales sobre las acciones de seguridad (uso adecuado de recursos, uso de claves, intentos fallidos, etc.), debe también aplicarse el monitoreo a usuarios privilegiados como administradores de BD, cambios de parametrizaciones contables, acciones de proveedores en ambientes de producción.	Procedimientos para revisión de log's	Gerencia de División de Informática / Seguridad Informática	Detectivo	Manual	Trimestral	Si	No	Débil
	19	Se maneja auditoría a nivel de base de datos solo para el usuario "sa", para los aplicativos de negocio la auditoria se programa en el propio aplicativo por lo que depende del técnico la implementación de la misma, situación que no refleja confiabilidad en los rastros obtenidos sea por error en la programación o porque no se la consideró incompleta o no se la consideró. No hay auditoria para consultas.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil

	20	Los aplicativos de negocio no tienen implementados las facilidades de alertas tempranas, es importante que se implementen alertas relacionadas al negocio como de seguridad.	Control procedimiental mediante reportes	Todas las áreas	Detectivo	Manual	Por demanda	Si	No	Débil
	21	Sólo algunos de los equipos tecnológicos tienen implementadas alertas tempranas (red, servidores - Inside Manager o Virtual Center vía correo. Las BD no tienen alertas.	Procedimiento de monitoreo	Gerencia de División de Informática	Detectivo	Automático	Constante	Si	No	Moderado
Control Accesos	22	La CFN tiene implementadas herramientas de Secure Login, Identity Manager y Novell (eDirectory) para manejar identificación y autenticación, sin embargo, la solución de seguridad no está integrada a todos los sistemas (Gestor-fiducia, Risk Control Services y Qlik View).	Aplicaciones de negocio integradas a IDM	Seguridad Informática	Preventivo	Manual	Constante	Si	No	Moderado
	23	La estructura de la contraseña (autenticación) no es estándar en todas las aplicaciones y sw (PCIE's no acepta caracteres especiales y es case-insensitive, COBIS no acepta caracteres especiales y es case-sensitive, Intranet acepta caracteres especiales y es case-sensitive, en algunas Pc's la clave del administrador esta en blanco.	Sincronización de claves (IDM)	Seguridad Informática	Preventivo	Manual	Constante	Si	No	Moderado
	24	Las características de la contraseña (autenticación) no son estándar y en algunos casos no son seguras, por ejemplo: Red y PCIE's v5 y 9 expira cada 30 días, v6 no expira, COBIS cada 60. Sólo la Red pide cambio de clave la primera vez o cuando el administrador resetea la misma. Sólo la Red y COBIS registra intentos fallidos y controlan contraseñas históricas. La Red, COBIS y PCIE's controlan el número de instancias. PCIE's no bloquean la cuenta luego de intentos fallidos de acceso. La Red y COBIS tienen administración de horarios.	Sincronización de claves (IDM), las demás característica s deben ser estandarizada s	Seguridad Informática	Preventivo	Manual	Constante	No	No	Débil

	25	Los mecanismos de autenticación están implementados dentro de los sistemas, es decir, los usuarios, claves y privilegios residen en tablas de BD. COBIS maneja 3DES. PCIE's registra contraseña plana (nadie tiene acceso a esta tabla sólo el adm de BD. El login de BD de PCIE's está encriptado.	Clave en PCIE's restringido el acceso de visualización. Cobis mecanismo seguro (core de negocio)	Gerencia de División de Informática	Preventivo	Manual	Constante	Si	No	Moderado
	26	Claves sensibles como la del administrador de BD, de servidores, elementos de comunicaciones son manejadas por una sola persona. Falta elaborar un procedimiento para manejo de claves sensibles.	Existe personal de backup tanto para Infraestructura de TI como de BD	Gerencia de División de Informática	Preventivo	Manual	Por demanda	No	No	Débil
	27	Es posible administrar los servidores desde cualquier PC, incluso desde sucursales. Se ha dado acceso remoto a proveedores de forma controlada. El soporte a usuarios se ejecuta mediante acceso remoto a las PC's que tiene la posibilidad de no solicitar aprobación al dueño del equipo.	Se permite la administración de servidores y Pc's con credenciales Contratos de soporte de proveedores (acceso controlado)	Gerencia de División de Informática	Preventivo	Manual	Por demanda	Si	No	Moderado
	28	Los servicios de seguridad perimetral están tercerizados por lo que debe existir acuerdos claros y documentados para de poder auditar y monitorear las acciones del proveedor	En el próximo contrato se dejará explícito las condiciones de auditoría y monitoreo	Gerencia de División de Informática / Seguridad Informática	Detectivo	Manual	Por demanda	Si	Si	Débil
	29	El área de auditoria informática no realiza pruebas de ethical hacking ni auditoria forense puesto que no está definido entre sus funciones. Se ha realizado un prueba de ethical hacking liderado por el área de Seguridad Informática	Ethical hacking externo; Análisis de vulnerabilidades; Revisión de	Seguridad Informática	Detectivo	Automático	Por demanda	Si	No	Moderado

			configuración básica de computadores							
	30	El sistema Informes Cobis es de reportería que tiene claves genéricas, se puede bajar a Excel y es utilizada por varias áreas como cartera, prevención de lavado de activos, planeación, etc. El personal de desarrollo usa ISQL para consultar data de producción. Para ambos casos no queda registro de la actividad del usuario	El registro queda en el log de la BD, aunque con un usuario genérico (ucobis, sa)	Gerencia de División de Informática	Detectivo	Manual	Constante	No	No	Débil
	31	Los cambios de roles por cambios administrativos son manuales por lo que a veces ciertos funcionarios se quedan con los privilegios de ambas funciones (anterior y nueva).	Norma interna de RRHH y Control de Accesos Reporte de RRHH Reporte de jefaturas Depuración periódica de usuarios/roles Campañas de concienciación	Subgerencia Nacional de RRHH y DO	Preventivo	Manual	Por demanda	Si	No	Moderado
	32	La administración total de los equipos tecnológicos está a cargo de la Gerencia de División de Informática, por lo que usuarios en servidores y base de datos creados por funcionarios de esta gerencia.	No existe		No aplica	No aplica	No aplica	No aplica	No aplica	Débil

Elaborado por: *Tania Guevara H.*

3.3.3.3. Actividad A3.3: Riesgo Residual

3.3.3.3.1. Tarea T3.1.1: Establecimiento de riesgo residual

El riesgo residual se determina por la combinación del riesgo total y el nivel de eficacia de los controles implementados conforme lo definido en el Anexo G – Criterios para calificar el riesgo residual (ver sección 2.3.5.1, tarea T3.1.3).

Los resultados del establecimiento de riesgo residual muestran al finalizar la tarea T4.1.1: Formular Planes de Mitigación de los Riesgos de la fase 4: Tratamiento de Riesgos.

3.3.3.4. Actividad A3.4: Seguimiento de avance

3.3.3.4.1. Tarea T3.4.1: Informe de seguimiento de avance

Tabla No 3.18: Acta de Reunión, evaluación de riesgos, informe seguimiento

Acta de Reunión

Fecha: Viernes, 30 de Septiembre del 2011

Participantes

Xxxxx Xxxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxxx	Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática

Asunto: Seguimiento de avance del proyecto de evaluación de riesgos de seguridad de la información

Temas tratados

- Se revisa el cumplimiento de las actividades detalladas en el cronograma de trabajo del proyecto correspondientes a la fase 3
- Se valida que no ha existido dificultades en el cumplimiento del cronograma
- A continuación se detalla cada tarea con el resumen de lo realizado:

Avance del Proyecto Evaluación de Riesgos de Seguridad de la Información	
Fase / Actividad / Tarea	**Avance**
Fase 3 – Evaluación de Riesgos / Actividad A3.1: Riesgo Bruto	
Tarea T3.1.1: Establecimiento de riesgo bruto	100% completado, se valida la correcta asignación de severidad del riesgo total.
Fase 3 – Evaluación de Riesgos / Actividad A3.2: Controles Existentes	
Tarea T3.2.1: Identificación de controles existentes Tarea T3.2.1: Valoración de controles existentes	100% completado, reuniones de trabajo con funcionarios encargados de la administración de los controles y auditoría interna, se complementa con la información relevada en entrevistas y documentación institucional.
Fase 3 – Evaluación de Riesgos / Actividad A3.3: Riesgo Residual	
Tarea T3.1.1: Establecimiento de riesgo residual	100% completado, se valida la correcta asignación del nivel riesgo residual.

- La fase 3 está concluida al 100%.

Resultados

Cronograma de trabajo actualizado con el porcentaje de avance del proyecto.

Firma de los participantes

Xxxxx Xxxxxxx Gerente Nacional de Riesgos	Xxxxx Xxxxxxx Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx Analista de Seguridad Informática	Xxxxx Xxxxxxx Analista de Seguridad Informática

Elaborado por: *Tania Guevara H.*

3.3.4. FASE 4: TRATAMIENTO DE RIESGOS

3.3.4.1. Actividad A4.1: Plan de Seguridad de la Información

3.3.4.1.1. T4.1.1: Formular Planes de Mitigación de los Riesgos

Los planes para mitigar los riesgos de seguridad de la información identificados, contemplan una serie de actividades y consideraciones que se recomienda ejecutar a fin de dar tratamiento a los riesgos latentes derivados de cada vulnerabilidad encontrada, su ejecución depende directamente de las decisiones que la administración de la CFN tome, es decir, depende de la tolerancia al riesgo institucional (ver sección 2.3.6.1, tarea T4.1.1).

Tabla No 3.19: Plan de Mitigación

Plan de Mitigación Corporación Financiera Nacional				
Dom	**No**	**Vulnerabilidad / Oportunidad de Mejora**	**Riesgo Residual**	**Plan de Mitigación**
Política Seguridad	1	Existe una política y tres normas de seguridad de la información institucional basada en la norma ISO/IEC 27001, las mismas que son revisadas periódicamente conforme una planificación. La política tiene definido sanciones por incumplimiento, al momento solo se ha sido necesario hacer llamados de atención. La mayoría de funcionarios conocen de la política la parte que les corresponde aplicar, sin embargo, sería importante hacer mayor difusión de la misma. Algunos funcionarios consideran que ponen en práctica ciertos aspectos de seguridad por cuenta propia, por ejemplo, escritorios limpios, dado que aprendieron en otras instituciones; consideran que este tema no forma parte de la política. (Oportunidad de Mejora)	No aplica	O1 - Continuar y profundizar la ejecución del Plan de Concienciación de Seguridad de la Información, enfatizando sobre la difusión de la política de seguridad direccionada al conocimiento que cada uno de los funcionarios debe conocer para una aplicación correcta de la misma, es decir, directrices generales para todos los funcionarios, directrices adicionales y específicas para propietarios de la información, personal de tecnología, recursos humanos, jefaturas, etc.
	2	Existen normas, estándares y procedimientos (operativos y técnicos) de seguridad, sin embargo, la documentación no es completa, faltaría documentar aspectos relacionados a evaluación de riesgos, gestión de incidentes de seguridad, etc. De igual forma, incluir seguridad en procedimientos relacionados, tales como, control y gestión de tecnología, por ejemplo, programación segura.	Superior	P1 - Elaborar la documentación complementaria de seguridad de la información: Normas y Estándares - que tiene relación con los 11 dominios propuestos por la Norma ISO/IEC 27001. Procedimientos e instructivos tanto técnicos como operativos en coordinación con la áreas competentes.
Seguridad RRHH	3	El proceso de selección de personal, no incluye una evaluación formal relacionada a investigación del aspirante (antecedentes). Algunos pasantes van a puestos críticos y no siguen el mismo procedimiento de selección, y no reciben inducción institucional.	Alto	P2 - El proceso de selección de personal debe garantizar la idoneidad en todos los aspectos del aspirante que ingresa a laborar en CFN, esto involucra a aspectos de importancia como el conocer el pasado laboral y relacionados del aspirante a fin de predecir en cierta forma su comportamiento y tendencias futuras relacionadas a la prevención de fraudes y espionaje principalmente; este tipo de procedimiento debería implementarse para puestos (funciones) críticos y debe constituir un elemento decisorio en la contratación. De igual forma debe restringirse la asignación de funciones críticas a personal que se encuentra en calidad de pasante, de ser el caso, este tipo de contrataciones debe tener la misma rigurosidad que se aplica a aspirantes de contrato.

	4	En algunas áreas se ha definido personal alterno que cuando está operando causa que no haya división de funciones, esto por falta de recursos, por ejemplo en tecnología y sucursales	Superior	P3 - Se debe definir personal alterno (backups) cuyas funciones no entren en conflicto de intereses, es decir, que de ninguna forma un mismo funcionario pueda cerrar un ciclo completo de un proceso o actividad. Complementariamente se debe garantizar que los perfiles adicionales autorizados se asignen únicamente por el período de tiempo de reemplazo. La Jefatura deberá vigilar constantemente al funcionario que está cumpliendo dos funciones a la vez. Como mejora del proceso se debe implementar un mecanismo por el cual el funcionario reemplazante suscriba un acuerdo de responsabilidad por las funciones adquiridas en el tiempo de reemplazo, es decir, se debe generalizar a todos los cargos, no solo en subrogaciones.
	5	Existe un programa de concienciación de seguridad de la información formal. Se ha dado capacitación en materia de seguridad, sin embargo, es importante validar que dicha capacitación haya llegado a todos los funcionarios	Moderado	O2 - Se debe continuar con la ejecución del programa de concienciación de concienciación en materia de seguridad de la información en coordinación con la Subgerencia Nacional de Recursos Humanos y Desarrollo Organizacional, el mismo que adicionalmente debe idearse otros mecanismos para llegar a los funcionarios como por ejemplo, inclusión de artículos de concienciación en revistas internas, evaluaciones periódicas para medir el nivel de concienciación (ingeniería social), etc.
	6	Existe conciencia que no se puede prestar el usuario/clave, pero se presentan casos en que se comparten claves por enfermedad, vacaciones, para soporte técnico. En el caso de mantenimiento de proveedores se presta el acceso (el funcionario escribe su clave, pero trabaja el proveedor). Algunos, luego de estos casos eventuales piden a seguridad cambio de clave.	Alto	P4 - En la ejecución del programa de concienciación de seguridad de la información se debe continuar recalcando la responsabilidad sobre la administración de credenciales (usuario/contraseña)
	7	Los funcionarios no bloquean sus PC's al abandonar su puesto de trabajo porque se bloquea automáticamente luego de un tiempo, adicionalmente, no dejan guardada documentación física sensible	Alto	P5 - Este riesgo obedece a la práctica de los funcionarios, por lo que para superarla es necesario implantar un cultura de seguridad y concienciar sobre las consecuencias que pueden derivarse del hecho de dejar desatendido el PC y/o documentación sensible, recordando al funcionario su responsabilidad sobre el uso de las credenciales, manejo de activos de información, etc., y, de ser necesario, aplicar las sanciones por incumplimiento a la política.
Comunicaciones y	8	Se maneja una red plana, sin segmentación de ningún tipo	Superior	P6 - Con el fin de resguardar servicios básicos tecnológicos, evaluar e implementar soluciones que permitan segmentar la red, por ejemplo, una red para el centro de cómputo o los servidores, firewalls internos, estas herramientas deben proveer alertas sobre las redes, etc. La implementación debe obedecer a un estudio previo a fin de implementar una arquitectura de red idónea para los servicios tecnológicos ofrecidos.

	9	La red de datos no tiene protección (cifrado) para el tránsito de información confidencial, de la misma forma información confidencial transmitida por correo electrónico no es cifrada.	Moderado	P7 - A fin de resguardar la información confidencial, se debe implementar un mecanismo o herramienta para cifrar la información, tanto en su tránsito por las redes sean públicas o privadas, como en su almacenamiento sea servidores, PC's, portables, bases de datos, correo electrónico, entre otros.
	10	Está permitido hacer administración remota de servidores vía VNC desde cualquier PC de la red, en algunos casos está configurado sin clave a pesar que los servidores siempre están bloqueados localmente.	Superior	P8 - Se debe evaluar e implementar una herramienta que permita realizar administración remota segura para servidores y equipos de la infraestructura tecnológica.
	11	Se encuentran desactualizadas los parches de las PC's, este proceso no se lo está ejecutando, no se cuenta con un laboratorio para validaciones previas.	Alto	P9 - El parchado en los equipos tecnológicos es un proceso que debe ejecutarse para garantizar su seguridad y apoyar a su correcto funcionamiento, sin embargo, se debe implementar un ambiente de pruebas en donde se valide que el parche a actualizar no daña la integridad y disponibilidad de los equipos, todo parche que sea liberado debe ser testeado en el ambiente de CFN previamente.
	12	Existe información crítica en los Pc's sin encriptar, por ejemplo, el personal alterno técnico cuando entra en funciones registra en un archivo (sin encripción) las contraseñas de administración de BD, a pesar de tener contraseña de acceso, el archivo no está encriptado.	Superior	P10 - Se debe asegurar la información que reside en PC's, para lo cual se debe evaluar e implementar una herramienta de cifrado de archivos; el uso adecuado de esta herramienta quedará bajo la responsabilidad de cada usuario y se debe reforzar su concienciación mediante campañas de seguridad.
	13	Para respaldo de información en estaciones de trabajo se ha implementado la herramienta iFolder, que su respaldo es manual, otras áreas (no del negocio) respaldan su información en discos externos. (Pasar a comunicaciones)	Moderado	O3 - Se debe concienciar sobre la importancia del respaldo de información sensible (cambio de cultura organizacional al respecto), o, evaluar otras herramientas que faciliten y automaticen el respaldo de la misma. Complementariamente se debe asegurar que información confidencial no sea respaldada en discos externos.
	14	La administración de base de datos no tiene una normativa definida en relación a la planificación de capacidad y rendimiento, esta actividad se la realiza conforme se presentan los requerimientos.	Superior	P11 - En forma general se debe complementar la documentación de normas, estándares, procedimientos e instructivos técnicos y operativos relacionados a la gestión tecnológica empezando por los de mayor sensitividad como por ejemplo la administración de base de datos (capacidad y rendimiento). Frente a la documentación que se elabore la Gerencia de División de Informática debe garantizar su aplicación.

	15	Los cortes de servicios informáticos prolongados en horarios laborales son eventuales (3 al año aproximado), sin embargo, por cierre de sistemas (cierre contable) no se cuenta con el servicio del sistema COBIS estable por dos días a fin de mes y se pierde tiempo de trabajo de los funcionarios de negocio. No hay Acuerdos de Niveles de Servicio definidos.	Superior	P12 - La Gerencia de División de Informática debe negociar los acuerdos de nivel de servicio SLA's con las diferentes áreas de la CFN y evaluar la forma de medir objetivamente el cumplimiento de los mismos. Complementariamente y a fin de garantizar la continuidad del negocio que se basa en tecnología, debe analizar el origen de los cortes de servicios informáticos, principalmente los relacionados con el sistema COBIS, tomar las acciones correctivas del caso e implementar las medidas preventivas. Se deberá buscar la estabilidad de todos los servicios (correo electrónico, sistemas de apoyo al core, internet, etc.)
	16	Falta desarrollar procedimientos para revisiones periódicas de pistas de auditoría, log's de seguridad y acciones de usuarios privilegiados.	Superior	P13 - Cada área competente debe elaborar sus procedimientos mediante los cuales ejecute los monitoreos regulares (pistas de auditoria para propietarios de la información y auditoria interna; log's de seguridad para seguridad informática), los procedimientos deben especificar el monitoreo de las acciones realizadas por usuarios con mayores privilegios.
	17	Debido a que la auditoria está implementada en el aplicativo, las pistas de auditoria no guardan la misma información para los eventos auditados, en otros casos no se audita el evento y en la mayoría no existe un reporte desde el aplicativo para ver dicha información.	Superior	P14 - Los propietarios de la información en coordinación con auditoria interna deben realizar un análisis integral de las necesidades de auditoria en los aplicativos del core de negocio, los resultados de dicho análisis deben ser implementados integralmente a fin auditar todos los eventos requeridos y estandarizar su almacenamiento; para la continuidad del proceso se debe revisar y de ser necesario modificar la metodología de proyectos y/o desarrollo de aplicaciones; estas metodologías deben garantizar la participación del personal requerido para que sus definiciones sean oportunas.
	18	Se hace monitoreo de usuarios funcionales sobre las acciones de seguridad (uso adecuado de recursos, uso de claves, intentos fallidos, etc.), debe también aplicarse el monitoreo a usuarios privilegiados como administradores de BD, cambios de parametrizaciones contables, acciones de proveedores en ambientes de producción.	Alto	P15 - Es necesario implementar monitoreos regulares en las diferentes áreas competentes, por ejemplo, se debe monitorear las actividades realizadas por usuarios técnicos con privilegios, usuarios funcionales responsables de ejecutar actividades críticas en los sistemas de información, etc. Para facilitar esta tarea será necesario automatizar los procesos de monitoreo para lo cual se debe evaluar e implementar una herramienta que en forma ideal brinde la funcionalidad de monitoreo desde una consola central permitiendo a los diferentes actores ejecutar sus monitoreos según su responsabilidad.

	19	Se maneja auditoría a nivel de base de datos solo para el usuario "sa", para los aplicativos de negocio la auditoria se programa en el propio aplicativo por lo que depende del técnico la implementación de la misma, situación que no refleja confiabilidad en los rastros obtenidos sea por error en la programación o porque no se la consideró incompleta o no se la consideró. No hay auditoria para consultas.	Superior	P16 - Se debe garantizar la integridad y permanencia para el almacenamiento de log's de seguridad y pistas de auditoria, ya que el guardar esta data en las tablas de base de datos es susceptible de manipulación; para el efecto se debe evaluar e implementar mecanismos seguros como una herramienta para el manejo centralizado de rastros para auditoria sea de base de datos, sistemas operativos, aplicaciones de negocio, servidores, equipos de comunicación, facilidades tecnológicas (correo electrónico), etc.
	20	Los aplicativos de negocio no tienen implementados las facilidades de alertas tempranas, es importante que se implementen alertas relacionadas al negocio como de seguridad.	Superior	P17 - Para facilitar el monitoreo de acciones de usuarios funcionales, usuarios privilegiados, patrones de conducta, etc., se debe implementar alertas tempranas tanto en los aplicativos de negocio como en las herramientas tecnológicas. La implementación de alertas tempranas adicional de facilitar el monitoreo y seguimiento de acciones de usuarios, también facilitan la gestión de actividades propias del negocio, transformándola en gestión proactiva. Para su definición deberán participar los propietarios de la información, personal técnico y de seguridades. Sería importante la participación de auditoría interna, sin embargo, no es requerida.
	21	Sólo algunos de los equipos tecnológicos tienen implementadas alertas tempranas (red, servidores - Inside Manager o Virtual Center vía correo. Las BD no tienen alertas.	Alto	P18 - Todo equipo tecnológico que soporte un servicio crítico debe tener implementado alertas tempranas a fin de garantizar la continuidad del servicio y por tanto del negocio. El complemento son los procedimientos, el entrenamiento y la capacidad de reacción del personal técnico para reaccionar adecuada y oportunamente frente a dichas alertas.
Control Accesos	22	La CFN tiene implementadas herramientas de Secure Login, Identity Manager y Novell (eDirectory) para manejar identificación y autenticación, sin embargo, la solución de seguridad no está integrada a todos los sistemas (Gestor-fiducia, Risk Control Services y Qlik View).	Bajo	O4 - Las herramientas de administración centralizada de seguridad (identidad) permite manejar de forma controlada el ciclo de vida de una cuenta/contraseña de usuario, considerando que la CFN ya tiene implementado un Identity Manager, es necesario fortalecerlo, para lo cual se debe integrar al mismo la mayoría de aplicaciones con énfasis en aplicaciones de negocio (debe responder a un análisis costo - beneficio), estandarizar la autenticación en las aplicaciones ya integradas, siendo de vital importancia la estandarización en aplicaciones que soportan el negocio (core de negocio), y, completar la automatización de todo el ciclo de vida de la identidad (creación, mantenimiento, baja) considerando que los actores requeridos deben ser involucrados (RRHH, propietarios de la información, seguridades, entre otros)

	23	La estructura de la contraseña (autenticación) no es estándar en todas las aplicaciones y sw (PCIE's no acepta caracteres especiales y es case-insensitive, COBIS no acepta caracteres especiales y es case-sensitive, Intranet acepta caracteres especiales y es case-sensitive, en algunas Pc's la clave del administrador esta en blanco.	Moderado	Aplicar la oportunidad de mejora O4.
	24	Las características de la contraseña (autenticación) no son estándar y en algunos casos no son seguras, por ejemplo: Red y PCIE's v5 y 9 expira cada 30 días, v6 no expira, COBIS cada 60. Sólo la Red pide cambio de clave la primera vez o cuando el administrador resetea la misma. Sólo la Red y COBIS registra intentos fallidos y controlan contraseñas históricas. La Red, COBIS y PCIE's controlan el número de instancias. PCIE's no bloquean la cuenta luego de intentos fallidos de acceso. La Red y COBIS tienen administración de horarios.	Alto	P19 - Para mitigar este riesgo se puede aplicar la oportunidad de mejora O4, o en su defecto, es necesario que los sistemas que soportan el core de negocio, en este caso el sistema COBIS y PCIE Riesgos se integren completamente al sistema Identity Manager y al LDAP (eDirectory) permitiéndolos manejar la autenticación; complementariamente, estos aplicativos de negocio deberán cumplir obligatoriamente lo dispuesto en la norma de seguridad relacionada con la Adquisición, Mantenimiento y Desarrollo de Sistemas.
	25	Los mecanismos de autenticación están implementados dentro de los sistemas, es decir, los usuarios, claves y privilegios residen en tablas de BD. COBIS maneja 3DES. PCIE's registra contraseña plana (nadie tiene acceso a esta tabla sólo el adm de BD. El login de BD de PCIE's está encriptado.	Moderado	Aplicar el plan de mitigación P19.
	26	Claves sensibles como la del administrador de BD, de servidores, elementos de comunicaciones son manejadas por una sola persona. Falta elaborar un procedimiento para manejo de claves sensibles.	Superior	P20 - Considerando que no sólo el área tecnológica maneja claves sensitivas, se debe normar los lineamientos para la administración de claves sensibles, mediante la elaboración de un procedimiento operativo, complementariamente es importante controlar periódicamente la correcta aplicación de dicho procedimiento, dicho control deberá estar a cargo de las jefaturas correspondientes y del área de seguridades.
	27	Es posible administrar los servidores desde cualquier PC, incluso desde sucursales. Se ha dado acceso remoto a proveedores de forma controlada. El soporte a usuarios se ejecuta mediante acceso remoto a las PC's que tiene la posibilidad de no solicitar aprobación al dueño del equipo.	Alto	P21 - Se debe limitar la posibilidad de administración de servidores y equipos de comunicación y seguridad definiendo los puntos (pc's) desde la cuales está permitido su acceso a fin de minimizar la probabilidad de acceso no autorizado y/o daños en la configuración, esta definición debe estar basada en una normativa de seguridad, una alternativa es implementar una solución NAC haciendo un análisis de costo/beneficio a fin de permitir acceso a la red y su administración únicamente a equipos controlados. La normativa de administración remota debe incluir la obligatoriedad de solicitar autorización del propietario del equipo (contraseña para servidores y aceptación del usuario para PC's)

	28	Los servicios de seguridad perimetral están tercerizados por lo que debe existir acuerdos claros y documentados para de poder auditar y monitorear las acciones del proveedor	Alto	P22 - Complementario al plan de mitigación P15 se debe monitorear periódicamente las actividades de proveedores cuando son los encargados de la administración de servicios, las evaluaciones servirán para validar si el proveedor está cumpliendo con las expectativas de la institución y se maneja conforme los acuerdos establecidos, por lo que es importante, suscribir SLA's y acuerdos que permitan dicho monitoreo.
	29	El área de auditoria informática no realiza pruebas de ethical hacking ni auditoria forense puesto que no está definido entre sus funciones. Se ha realizado un prueba de ethical hacking liderado por el área de Seguridad Informática	Alto	P23 - A fin de garantizar evaluaciones de seguridad independientes, se debe revisar las funciones del área de auditoria informática, de ser el caso, complementarlas para que incluya auditoria de los procesos de seguridad y llevar a cabo análisis de vulnerabilidades (ethical hacking) y auditoría forense interna (sin arrogarse funciones de otras entidades como la fiscalía)
	30	El sistema Informes Cobis es de reportería que tiene claves genéricas, se puede bajar a Excel y es utilizada por varias áreas como cartera, prevención de lavado de activos, planeación, etc. El personal de desarrollo usa ISQL para consultar data de producción. Para ambos casos no queda registro de la actividad del usuario	Superior	P24 - Se debe evaluar mecanismos efectivos para el control sobre consultas de información clasificada como confidencial. Los principales controles a implementar deben ser: implementar seguridades en el sistema Informes Cobis que incluya la administración de identificación, autenticación y autorización principalmente; para el personal de desarrollo se debe quitar los privilegios de consulta en el ambiente productivo, sobre la base de que existe suficiente personal y separación de funciones.
	31	Los cambios de roles por cambios administrativos son manuales por lo que a veces ciertos funcionarios se quedan con los privilegios de ambas funciones (anterior y nueva).	Moderado	Aplicar la oportunidad de mejora O4.
	32	La administración total de los equipos tecnológicos está a cargo de la Gerencia de División de Informática, por lo que usuarios en servidores y base de datos creados por funcionarios de esta gerencia.	Superior	Aplicar el plan de mitigación P20.

Elaborado por: *Tania Guevara H.*

3.3.4.1.2. Tarea T4.1.2: Formular el Plan de Seguridad de la Información

El Plan de Seguridad de la Información[34], es un documento que organiza los planes de mitigación en proyectos de Seguridad Institucional, contempla los responsables, niveles de aprobación, objetivos generales, su alineación con las estrategias de la CFN, recursos requeridos, indicadores de cumplimiento; por cada proyecto se detallan objetivos, impacto estratégico, nivel de esfuerzo, riesgo, responsables, restricciones y limitaciones, supuestos, presupuesto, recursos y tiempo estimado (ver sección 2.3.6.1, tarea T4.1.2).

3.3.4.2. Actividad A4.2: Aprobación interna

3.3.4.2.1. Tarea T4.2.1: Aprobación interna del Plan de Seguridad de la Información

Los detalles de esta actividad se describen la sección 2.3.6.2.

Tabla No 3.20: Acta de Reunión, aprobación interna del plan de seguridad

Acta de Reunión

Fecha: Jueves, 13 de Octubre del 2011

Participantes

Xxxxx Xxxxxxx	Gerente Nacional de Riesgos
Xxxxx Xxxxxxx	Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx	Analista de Seguridad Informática

Asunto: Aprobación del plan de seguridad de la información

Temas tratados

- El responsable del área de Seguridad Informática presente el plan de seguridad.

[34] Plan de Seguridad de la Información, se encuentra detallado en el documento PlanSeguridadInformacion.doc adjunto.

- El equipo de trabajo revisa detalladamente la propuesta con énfasis en los proyectos, responsables, presupuesto y tiempos.
- El Gerente Nacional de Riesgos da por conocido y aprobado el plan presentado

Resultados

Plan de seguridad de la información aprobado por la Gerencia Nacional de Riesgos.

Firma de los participantes

Xxxxx Xxxxxxx Gerente Nacional de Riesgos	Xxxxx Xxxxxxx Jefe Nal. de Seguridad Informática
Xxxxx Xxxxxxx Analista de Seguridad Informática	

Elaborado por: *Tania Guevara H.*

3.3.4.3. Actividad A4.3: Aprobación de la Dirección

3.3.4.3.1. Tarea T4.3.1: Aprobación del Plan de Seguridad de la Información por parte del CAIR y de la Dirección

El plan de seguridad de la información fue conocido y aprobado en sesión del Comité de Administración Integral de Riesgos – CAIR celebrada el 20 de octubre del 2011, en este comité participó la Alta Dirección de la CFN (Presidente, Gerente General). Los detalles de esta actividad se describen la sección 2.3.6.3.

CAPITULO IV. MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN FINANCIERA NACIONAL

4.1. INTRODUCCIÓN

El diseño de un Modelo de Gestión de Seguridad de la Información para la CFN basado en una metodología propia de Gestión de Riesgos, permitirá entre otros aspectos importantes, cumplir con la normativa y requerimientos regulatorios de los diferentes organismos de control, proteger adecuadamente los activos de información de posibles amenazas y vulnerabilidades, garantizar que se cumplan los objetivos básicos de la seguridad de la Información como son la confidencialidad, integridad y disponibilidad, y apoyar a la continuidad del negocio.

La norma ISO 27001:2005 es un estándar internacionalmente aceptado, orientado al diseño, implementación y certificación de un Sistema de Gestión de Seguridad de la Información (SGSI) adaptable a la realidad de las diferentes industrias sin importar su tamaño, por este motivo el Instituto Ecuatoriano de Normalización – INEN la ha adoptado como norma técnica ecuatoriana[35], habiendo acogido hasta el momento las siguientes normas de la familia ISO 27000:

- NTE INEN-ISO/IEC 27000:2012 - Tecnología de la información - Técnicas de seguridad - Sistema de gestión de seguridad de la información - Descripción general y vocabulario
- NTE INEN-ISO/IEC 27001:2011 - Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos

[35] Instituto Ecuatoriano de Normalización, http://www.inen.gob.ec/index.php?option=com_content&view=article&id=206&Itemid=62, consultado en agosto del 2012.

- NTE INEN-ISO/IEC 27002:09 - Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información
- NTE INEN-ISO/IEC 27003:2012 - Tecnología de la información - Técnicas de seguridad - Guía de implementación del sistema de gestión de la seguridad de la información
- NTE INEN-ISO/IEC 27004:2012 - Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información – Medición
- NTE INEN-ISO/IEC 27005:2012 - Tecnología de la información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información
- NTE INEN-ISO/IEC 27006:2012 - Tecnología de la información. Técnicas de seguridad. Requisitos para organizaciones que proveen auditoría y certificación de sistemas de gestión de la seguridad de la información

4.2. OBJETIVOS

- Diseñar un modelo de gestión de seguridad de la información aplicable a la Corporación Financiera Nacional, el mismo que deberá contemplar al menos:
    - Los requerimientos de documentación institucional de seguridad de la información necesarios para gestionar adecuadamente la seguridad de la información
    - Un programa de concienciación del personal en materia de seguridad
    - Una declaración de aplicabilidad sobre la tecnología a contralar
- Analizar y validar la aplicabilidad de la propuesta

4.3. ESTRUCTURA DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.3.1. ALINEACIÓN DEL MODELO CON NORMAS INTERNACIONALES Y CON LA CULTURA ORGANIZACIONAL DE CFN

El modelo de Gestión de Seguridad de la Información debe contemplar todos los elementos necesarios para crear, implantar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)[36] aplicable a la realidad de la CFN que viabilice el cumplimiento de los requerimientos de seguridad de la Institución.

Considerando que la Corporación Financiera Nacional cuenta con certificación ISO 9001:2000 y con el objeto futuro de lograr una certificación en materia de Seguridad de la Información, el modelo de gestión propuesto se basará principalmente en la norma ISO/IEC 27001:2005.

La estrategia referida allanará el camino a la certificación deseada puesto la norma ISO/IEC 27001:2005 sigue las pautas marcadas en la ISO 9001:2000, lo cual asegura una implementación integrada y consistente, el control de documentación que hacen referencia a la creación, modificación, actualización, aprobaciones, versiones, entre otros, son procesos que ya están instaurados en CFN y forma parte de su cultura organizacional.

4.3.2. MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN MEJORA CONTINUA

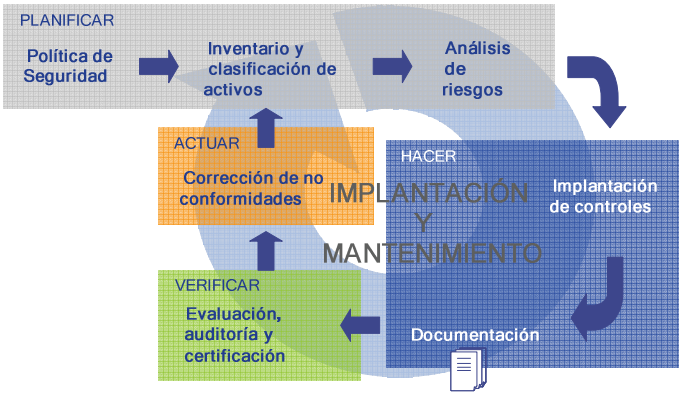
Para la implementación del modelo de gestión de seguridad de la información, el proceso utilizado se enfoca en el Ciclo de Deming - PDCA[37] como un requisito general.

---

[36] UNE-ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información (SGSI) Requisitos, página 7.

[37] Ciclo de Deming: Plan – Do – Check - Act

Figura No 4.1: Modelo de aseguramiento continuo de la información



Fuente: *Plan Estratégico de Tecnología de la Información CFN*

Elaborado por: *Tania Guevara H.*

4.3.2.1. Planificar

Parte por la definición de la política, normas, procesos y procedimientos del SGSI necesarios para gestionar los riesgos y mejorar la seguridad de la información, alineados a la política y objetivos Institucionales.

4.3.2.2. Hacer

Consiste en implementar tanto la política, normas, procesos, procedimientos del SGSI como los controles definidos fruto del análisis de riesgos.

4.3.2.3. Verificar

Es evaluar la eficacia y eficiencia de la política, normas, procesos, procedimientos y controles implementados, normalmente se lo viabiliza con auditorías, sus resultados deben ser informados a la Alta Gerencia para su revisión.

4.3.2.4. Actuar

Pretende adoptar las medidas preventivas y correctivas en función de los resultados de la verificación del SGSI, considera adicionalmente información relevante para mejorar el cumplimiento de los requerimientos de seguridad de la información definidos por el negocio y por órganos de control, complementariamente permite que el sistema se adapte a los principales cambios internos y externos de la Institución.

4.3.3. ELEMENTOS DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En concordancia con los requerimientos de la norma ISO/IEC 27001:2005, el modelo de gestión de seguridad de la información propuesto se enfocará fundamentalmente en los siguientes elementos:

Figura No 4.2: Elementos del Modelo de Gestión de Seguridad de la Información

Elaborado por: *Tania Guevara H.*

- Gestión de Riesgos de Seguridad de la Información, basado en:
    - Activos de Información, ponderados por Confidencialidad, Integridad y Disponibilidad (CID)
    - Requerimientos de seguridad del negocio, relacionados con dominios de la norma ISO/IEC 27001:2005
- Cuerpo normativo - documentación, que incluye:
    - Alcance del SGSI
    - Política de Seguridad
    - Metodología de Gestión de Riesgos de Seguridad de la Información
    - Plan de Seguridad - Plan de tratamiento de los riesgos identificados
    - Procesos, procedimientos y registros operativos de seguridad
    - Declaración de aplicabilidad DDA
- Responsabilidades de la Dirección
    - Compromiso y gestión de recursos
    - Formación y concienciación en materia de seguridad de la información
    - Revisión del SGSI
- Ejecución de procesos y controles
    - Ejecución del Plan de Seguridad
    - Implementación de controles
    - Auditorías y mejora del SGSI

La adecuada gestión de todos los elementos descritos apoyan directamente a la continuidad del negocio, este elemento forma parte intrínseca del SGSI al ser uno de los once dominios de la norma ISO/IEC 17799:2000 – Tecnología de Información. Código de Prácticas para la Gestión de Seguridad de la Información, que corresponde al Anexo A de la norma ISO/IEC 27001:2005.

Un proceso importante es el control de documentos y registros operativos, que en Corporación Financiera Nacional está operativo ya que se integraría con el proceso de gestión de calidad ISO 9001.

4.4. PROCESOS PARA LA IMPLEMENTACIÓN DEL MODELO DE GESTION DE SEGURIDAD DE LA INFORMACIÓN EN LA CFN

4.4.1. GESTIÓN DE RIESGOS

Toda implementación de un Sistema de Gestión de Seguridad de la Información debe partir del hecho de conocer de manera objetiva el estado de seguridad de la Institución, en este contexto, es indispensable ejecutar un primer análisis y evaluación de riesgos.

En el capítulo 3 del presente trabajo de tesis, se ha realizado el primer ejercicio de gestión de riesgos, conforme la metodología planteada en el capítulo 2 de este documento, sus resultados proveen un conjunto medidas de seguridad que son necesarias implementar para alcanzar un nivel de riesgo aceptable definido por la Dirección[38].

El enfoque de evaluación de riesgos requerido por la norma ISO/IEC 27001:2005, contempla la definición de criterios para la estimación y aceptación del riesgo, identificación del riesgo, análisis y valoración del riesgo, tratamiento del riesgo, selección de controles y aprobación de la Dirección; este enfoque se alinea perfectamente con la metodología propuesta, conforme se muestra a continuación:

---

[38] A efectos prácticos de la Corporación Financiera Nacional, la Dirección se refiere a la Gerencia General, quien se apoyará en las recomendaciones de un Comité o cuerpo colegiado especialista en temas de Gestión de Riesgos y/o Gestión de Tecnología

4.4.1.1. Criterios para la estimación y aceptación del riesgo

Establecidos en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

Tabla No 4.1: Correlación de criterios de estimación y aceptación del riesgo

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Criterios para estimación del riesgo	Anexo E – Criterios para Calificar el Riesgo Bruto
	Anexo G – Criterios para Calificar el Riesgo Residual
Criterios para aceptación del riesgo	Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información Tarea T4.1.2: Formular el Plan de Seguridad de la Información[39] * Los criterios para la aceptación del riesgo también deberán ser incluidos en la Política de Seguridad tal como lo establece la norma internacional

Elaborado por: *Tania Guevara H.*

4.4.1.2. Identificación del riesgo

Establecidos en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

[39] La Metodología de Gestión de Riesgos de Seguridad de la Información, orienta a formular un Plan de Seguridad considerando los riesgos calificados como “Superior” y “Alto”

Tabla No 4.2: Correlación en identificación del riesgo

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Identificar activos y propietarios de información	Fase 2: Análisis de riesgos Actividad A2.1: Determinación de activos Tarea T2.1.1: Identificación de activos de información Tarea T2.1.2: Valoración de activos de información
Identificar amenazas	Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.2: Identificación de amenazas
Identificar Vulnerabilidades	Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.1: Identificación de vulnerabilidades
Identificar Impactos	Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.4: Estimación del impacto

Elaborado por: *Tania Guevara H.*

La metodología de riesgos de seguridad de la información, propone al contrario de lo estipulado en la ISO/IEC 27001:2005, primero estimar las vulnerabilidades y luego las amenazas, considerando que si no se tiene una vulnerabilidad, las amenazas no pueden ser explotadas, por tanto, solo se enfocará en analizar las amenazas reales a la institución.

4.4.1.3. Análisis y valoración del riesgo

Establecidos en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

Tabla No 4.3: Correlación en análisis y valoración del riesgo

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Evaluar la probabilidad	Fase 2: Análisis de riesgos Actividad A2.3: Identificación de riesgos Tarea T2.3.3: Estimación de probabilidad
Estimar el nivel de riesgo	Fase 3: Evaluación de riesgos Actividad A3.1: Riesgo bruto Actividad A3.3: Riesgo Residual
Validación con criterios de aceptación del riesgo	Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información

Elaborado por: *Tania Guevara H.*

4.4.1.4. Tratamiento del riesgo

Implícitos en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

Tabla No 4.4: Correlación en tratamiento del riesgo

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Aplicar controles (mitigar) Asumir el riesgo (aceptar) Evitar el riesgo (eliminar)	Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información

Transferir el riesgo	(selección de controles y aprobación de la dirección)

Elaborado por: *Tania Guevara H.*

4.4.1.5. Selección de objetivos de control y controles

Implícito en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

Tabla No 4.4: Correlación en selección de objetivos de control y controles

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Selección de objetivos de control y controles	Fase 4: Tratamiento de riesgos Actividad A4.1: Plan de Seguridad de la Información (selección de controles)

Elaborado por: *Tania Guevara H.*

4.4.1.6. Aprobación de la dirección

Establecido en la metodología de gestión de riesgos propuesta de acuerdo a la siguiente correspondencia:

Tabla No 4.5: Correlación en aprobación de la dirección

Norma ISO/IEC 27001:2005	**Metodología de Gestión de Riesgos propuesta**
Aprobación de la dirección	Fase 4: Tratamiento de riesgos Actividad A4.3: Aprobación de la Dirección

Elaborado por: *Tania Guevara H.*

4.4.2. DEFINICIÓN DE DOCUMENTACIÓN DE ALTO NIVEL

4.4.2.1. Alcance del SGSI

El alcance del SGSI estará determinado por el alcance del primer análisis y evaluación de riesgos que se lleve a cabo, para el caso de la Corporación Financiera Nacional, el alcance cubre al proceso primordial del negocio "Concesión de Crédito".

Las áreas involucradas directamente son Crédito de Primer Piso, Segundo Piso, Transporte y Comercio Exterior, e indirectamente, las áreas de apoyo que tienen relación con los dominios, objetivos de control y controles del Anexo A de la norma ISO/IEC 27001:2005.

4.4.2.2. Política de Seguridad

La Política propiamente dicha, es un documento de alto nivel, el cual contiene lineamientos de ámbito general, por ejemplo, al referirse al dominio de "Seguridad Física y Ambiental" en las características físicas del centro de cómputo, no indicará el nivel de temperatura o humedad específico que debe tener dicho espacio, sólo se referirá a que deberá estar protegido de los peligros ambientales.

Por otro lado, las Normas de Seguridad, sin dejar de ser generales, son las llamadas a detallar todo lo necesario en su ámbito de acción, es decir, se escribirá una norma por cada dominio de la norma internacional ISO/IEC 27001:2005, 11 en total, en las que se ampliará la política a fin de especificar características sean administrativas o incluso técnicas.

Complementariamente, es importante que exista definición de estándares, los cuales serán derivados de las normas que se establezcan, dicho documento facilita la labor de implementación de controles y validación de cumplimiento.

En el caso de la Corporación Financiera Nacional, se cuenta con un Manual de Seguridad de la Información que contiene Políticas, Normas y Estándares de Seguridad de la información, del análisis realizado, dicho manual en su mayoría cumple con los requerimientos de la norma ISO/IEC 27001:2005.

Se validó que la Política declara los siguientes aspectos exigidos por la norma internacional: objetivos, principios, niveles de aprobación, por tanto está alineada a la gestión de riesgos realizada quedando únicamente por actualizar la declaración explícita de los criterios de aceptación del riesgo.

4.4.2.3. Programa de Formación y Concienciación

En materia de seguridad de la información, la CFN cuenta con un Programa de Concienciación de Seguridad de la Información que contiene: responsables, concepto general, alineación con la estrategia Institucional, objetivos, importancia, elementos, alcance, audiencia, estrategias, planificación e indicadores.

Dicho programa es ejecutado en coordinación con el área de Recursos Humanos, quien es el responsable directo de todo lo relacionado con capacitaciones, sin embargo, se apoya con las diferentes áreas especialistas en cada temática.

En el Anexo H se encuentra el Programa de Formación y Concienciación en materia de seguridad de la información.

4.4.2.4. Declaración de Aplicabilidad

La declaración de aplicabilidad proporciona un resumen de las decisiones relativas al tratamiento de riesgos, para el presente trabajo de tesis en el Anexo I – Declaración de Aplicabilidad se detallan los controles existentes y

los seleccionados enmarcados en el alcance de la gestión de riesgos realizada.

4.4.3. APROBACIONES DE LA DIRECCIÓN

Conforme lo dispuesto en la Política de Seguridad de la Información de CFN, se ejecutan los siguientes niveles de revisión y aprobación:

- El Comité de Administración Integral de Riesgos deberá evaluar las políticas, normas y procedimientos recomendadas por el Área de Seguridad Informática, y proponer su aprobación a las instancias competentes.
- La Gerencia General aprobará las normas y procedimientos de Seguridad de la Información.
- El Directorio de la Corporación Financiera Nacional aprobará las Políticas de Seguridad de la Información[40]

4.4.3.1. Visto bueno para implantar y operar el SGSI

Toda iniciativa en materia de Seguridad de la Información debe estar avalada por la Dirección, por tanto, para implantar y mantener un Sistema de Gestión de Seguridad de la Información se debe gestionar su aprobación al más alto nivel, en caso de la Corporación Financiera Nacional le corresponde al Directorio declarar explícitamente su conformidad, autorización y apoyo para la constitución de un SGSI.

Obtener el visto bueno por parte de Directorio, constituye un factor indispensable y crítico de éxito, debido a que la seguridad no depende de un funcionario o un área específica en la Institución; su éxito se fundamenta en la colaboración activa del recurso humano expresada directamente en su accionar, en la adecuación y control de los recursos

[40] Política de Seguridad de la Información – CFN, página 4.

tecnológicos, y, en la disponibilidad de recursos tanto financieros como humanos que viabilicen los proyectos de seguridad.

4.4.4. IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

4.4.4.1. Ejecución del plan de seguridad

El plan de seguridad de la información, provee una serie de proyectos que permiten de alguna manera eliminar, mitigar o transferir los riesgos identificados.

Cada proyecto puede involucrar la implementación de un número elevado de controles, que a su vez podría suponer un impacto considerable sobre procesos y sistemas, por tal motivo, es necesario dedicar recursos suficientes para su gestión, con la finalidad de garantizar su coordinación y la calidad del resultado final[41].

4.4.4.2. Implementación de controles

La implementación de controles prioritarios se cubre con la ejecución del plan de seguridad de la información, ya que corresponden a controles identificados y destinados para cubrir vulnerabilidades fruto del análisis y evaluación de riesgos, sin embargo, pueden existir controles que son necesarios implementar para obtener la certificación deseada, pero, que no fueron identificados previamente.

Por este motivo, este paso adicional es necesario, su ejecución se sustenta en el documento de aplicabilidad DDA levantado como parte del proceso de planeación del SGSI.

---

[41] Juan Matalobos, Análisis de Riesgos de Seguridad de la Información, página 167.

4.4.4.3. Determinación de cómo medir la eficacia de los controles

La seguridad de la información en su mayoría es abstracta, invertir en seguridad muchas veces puede interpretarse como un gasto y no como una inversión para la prevención y/o control de incidentes penosos o costosos.

Implantar seguridad en una Institución es ciertamente costosa, implantar y operar un SGSI no es la excepción, por todo el proceso asociado: análisis y evaluación de riesgos, ejecución del plan de seguridad, implementación de controles, formar y concienciar al personal, etc.

En este sentido, se debe proporcionar a la Institución información sobre su eficacia y utilidad, esto se lo logra determinando métricas para evaluar sus resultados.

Complementariamente, existen beneficios al elaborar métricas en materia de seguridad de la información como son:

- Disponer información actualizada sobre la ejecución de proyectos, relacionadas al cumplimiento de presupuesto y tiempos[42].
- Validar del grado de consecución de objetivos, ya sea en relación a los requerimientos de seguridad, necesidad de cubrir riesgos o cumplir con organismos de control
- Validar el cumplimiento de políticas de seguridad institucionales
- Conocer de manera objetiva el nivel de madurez en materia de seguridad
- Comparar el nivel de seguridad con instituciones similares[43]

---

[42] Juan Matalobos, Análisis de Riesgos de Seguridad de la Información, página 168

[43] Ídem

Para el establecimiento de métricas se debe considerar los siguientes aspectos[44]:

- Definir el o los objetivos de la medición
- Los indicadores pueden cambiar en el corto, mediano y largo plazo
- Identificar un conjunto reducido de indicadores relevantes que permitan obtener información precisa
- Establecer mecanismos tecnológicos de preferencia y operativos que permitan realizar el cálculo de los indicadores de manera rápida y objetiva
- Establecer los parámetros aceptables de desempeño y las posibles desviaciones que sugieren revisar la implementación del control

4.4.4.4. Ejecución del Programa de Formación y Concienciación

El Programa de Formación y Concienciación en materia de Seguridad de la Información debe formar parte integral de la planificación de seguridad, constituye una herramienta de apoyo importante e indispensable para mejorar el nivel de madurez respecto a la seguridad de los funcionarios de una institución.

Los principales objetivos de ejecutar un programa para la formación y concienciación de seguridad de la información son[45]:

- Comunicar a los funcionarios sobre la importancia de proteger la información institucional
- Lograr que los funcionarios magnifiquen su responsabilidad respecto a la protección de la confidencialidad, integridad y disponibilidad de los activos de información

---

[44] ¿Cómo hacer un plan de trabajo?, http://axeleratum.com/2012/icomo-hacer-un-plan-de-trabajo-establecimiento-de-metricas/#, consultado en septiembre del 2012

[45] Programa de concienciación de seguridad de la información – CFN

- Fomentar una cultura de seguridad que convierta a los funcionarios en la primera barrera de seguridad de la información
- Lograr que los funcionarios comprendan que la seguridad no es sólo competencia de los especialistas en seguridad o personal técnico
- Formar y concienciar sobre el uso seguro y responsable de la tecnología

Es importante adicionalmente que el programa de formación y concienciación de seguridad de la información establezca sus propias métricas para establecer su eficacia.

4.4.4.5. Gestionar los incidentes de Seguridad de la Información

Una gestión adecuada de incidentes de seguridad de la información es indispensable en el establecimiento y operación de un SGSI, su objetivo es prevenir y limitar el impacto de los mismos[46].

Un incidente de seguridad es un evento adverso inesperado o no deseado en un sistema de cómputo que amenaza la confidencialidad, integridad, disponibilidad y/o confiabilidad de la información, y tiene una probabilidad significativa de comprometer las operaciones del negocio[47].

En el marco de un SGSI, la gestión de incidentes de seguridad debe contemplar al menos:

- La inclusión del dominio en la política de seguridad de la información
- La elaboración de normas y estándares
- La elaboración de procedimientos que contemple al menos:

---

[46] Política de Gestión de Incidentes de Seguridad de la Información, http://www.agesic.gub.uy/innovaportal/file/1217/1/politica_de_gestion_de_incidentes.pdf, consultado en septiembre de 2012.

[47] Política de Seguridad de la Información – CFN, página 2.

- Notificación / reporte del incidente
- Análisis e identificación inicial de causas
- Notificación inicial
- Recolección de pistas de auditoría o log's de seguridad (evidencia)
- Planificación e implementación de solución (es)
- Comunicación a afectados
- Notificación a la autoridad pertinente
- Seguimiento a implementación de solución definitiva (si aplica)

4.4.5. SUPERVISIÓN Y REVISIÓN DEL SGSI

4.4.5.1. Ejecución de procesos de supervisión y revisión

El proceso de supervisión y revisión de la eficacia del SGSI, es indispensable en el marco de aplicar la mejora continua, entre sus objetivos más relevantes podemos mencionar a[48]:

- Detectar tempranamente errores o debilidades del sistema de seguridad
- Permitir que la Dirección determine el cumplimiento de las políticas de seguridad institucional en relación a la ejecución correcta de actividades delegadas
- Ayudar a la detección de eventos y prevención de incidentes de seguridad, basado en indicadores
- Determinar la eficacia de los controles en base al cumplimiento de los requisitos de seguridad, y, de las acciones tomadas al resolver una violación de seguridad

[48] UNE-ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información (SGSI) Requisitos, página 12.

A continuación se listan las actividades que permiten llevar a cabo el proceso de supervisión y revisión del SGSI:

- Auditorías internas y externas periódicas
- Análisis y evaluación de riesgos periódicos
- Mediciones de eficacia de controles
- Revisión de cumplimiento de la política y normativa de seguridad
- Evaluaciones de gestión de incidentes

4.4.5.2. Medición de la eficacia

La medición de la eficacia debe ser ejecutada bajo los parámetros definidos en el punto 1.4.4.3 - Determinación de cómo medir la eficacia de los controles, que busca definir los indicadores que evalúen la vigencia y aplicabilidad de los controles implementados. Complementariamente, se debe evaluar los resultados de los indicadores descritos en el programa de formación y concienciación.

La eficacia global del SGSI está determinado por los resultados de auditorías, incidentes, indicadores de eficacia de controles, nivel de cumplimento de la política de seguridad institucional.

4.4.5.3. Evaluaciones de riesgos

El análisis y evaluación de riesgos de seguridad de la información es la base para una adecuada gestión de seguridad, principalmente debido a que la exposición a los riesgos de seguridad de la información cambia constantemente con la evolución de la tecnología, de la institución y de su entorno.

En tal sentido, es necesario planificar evaluaciones de riesgo periódicas que permitan mantener vigentes los proyectos y planes de seguridad, a fin

de garantizar que el esfuerzo empleado en la realización del análisis de riesgos no quede obsoleto en un período breve de tiempo[49].

Complementario a la ejecución integral de gestión de riesgos, se debe incorporar actividades de análisis de riesgos en el proceso de gestión de cambios y en la metodología de proyectos informáticos, para facilitar el proceso global es importante pensar en automatizarlo.

4.4.5.4. Auditorías

El proceso de supervisión y revisión del SGSI se apoya fuertemente en la ejecución de auditorías periódicas tanto internas como externas, debido a la necesidad de validar el cumplimiento de políticas, normas, estándares y procedimientos de seguridad desde una óptica independiente, objetiva e imparcial.

La ejecución de auditorías permitirá determinar si los objetivos de control, controles, procesos y procedimientos de seguridad del SGSI:

- Cumplen con lo establecido en: la norma ISO/IEC 27001:2005, las disposiciones de organismos de control, y, los requisitos de seguridad identificados,
- Se implantan y mantienen de forma efectiva y dan el resultado esperado

Todo el proceso de auditorías debe estar documentado, para la Corporación Financiera Nacional, este proceso deberá apegarse a lo establecido en el proceso de gestión de calidad ISO 9001.

---

[49] Juan Matalobos, Análisis de Riesgos de Seguridad de la Información, página 163

4.4.5.5. Revisión de la gestión de incidentes

La revisión de la gestión de incidentes aporta significativamente en la determinación del estado o nivel de seguridad, es un insumo importante en el proceso de supervisión y revisión del SGSI puesto que permite adoptar medidas preventivas y correctivas sobre debilidades tanto del sistema como de controles técnicos o administrativos.

4.4.5.6. Revisión de resultados por parte de la Dirección

Las revisiones de eficacia del SGSI son de responsabilidad de la Dirección y deben ser ejecutadas periódicamente (al menos una vez al año, conforme indica la norma ISO/IEC 27001:2005), para el efecto se deberá considerar los resultados del proceso de supervisión y revisión del SGSI, adicionalmente:

- Sugerencias y recomendaciones de mejora
- Acciones de seguimiento de revisiones anteriores
- Técnicas, productos o procedimientos para mejorar el SGSI
- Cualquier cambio que pueda afectar al SGSI

Producto de la revisión del SGSI por parte de la Dirección se cuenta con decisiones y acciones para actualizar el plan de seguridad, mejorar el SGSI, dotar de recursos, modificar: procedimientos, controles, modo de medir la eficacia de controles, entre otros.

4.4.5.7. Actualización del Plan de Seguridad

La actualización del plan de seguridad de la información es una actividad constante, fruto de la revisión del SGSI, de evaluaciones de riesgos, de ejecuciones de pruebas de vulnerabilidad o intrusiones, entre otros, incluso la ejecución de proyectos institucionales podrían sugerir cambios en la

planificación de seguridad, sea añadiendo o eliminando proyectos o simplemente modificando su priorización.

De cualquier modo, la actualización del plan de seguridad es una buena práctica de vital importancia para garantizar su vigencia y aplicabilidad.

4.4.6. MANTENIMIENTO Y MEJORA DEL SGSI

Un SGSI se mantiene y mejora mediante la aplicación de las siguientes acciones:

- Implementación de las medidas correctivas (eliminación de causas de no conformidades), preventivas (eliminación de posibles no conformidades) y mejoras identificadas
- Validación del logro de objetivos previstos
- Comunicación – difusión sobre las acciones tomadas

4.5. CONSIDERACIONES DEL MODELO DE GESTIÓN DE SEGURIDAD DELA INFORMACIÓN

4.5.1. REQUERIMIENTOS DE DOCUMENTACIÓN

La implementación de un SGSI conforme la norma ISO/IEC 27001:2005, supone la elaboración y mantenimiento de la siguiente documentación:

- Política de Seguridad de la Información, formalmente aprobada y difundida
- Definición del alcance del SGSI
- Procedimientos y mecanismos de control que soportan al SGSI
- Metodología de riesgos
- Informes de la gestión de riesgos
- Plan de Seguridad de la Información

- Procedimientos de operación y control de la gestión de seguridad y la descripción de indicadores para la medición de la eficacia de los controles
- Registros operativos
- Declaración de aplicabilidad

4.5.2. CUERPOS COLEGIADOS

4.5.2.1. Comité de Tecnología

El Comité de Tecnología de la Corporación Financiera Nacional, tiene entre sus responsabilidades el control y mantenimiento del plan de tecnología de información que deberá observar la política de seguridad de la información, a fin de garantizar[50]:

- La continuidad de las operaciones
- El proceso de adquisición, desarrollo, implementación y mantenimiento de aplicaciones
- El mantenimiento y operatividad de la infraestructura tecnológica
- La provisión de recursos y servicios informáticos de terceros
- La confidencialidad, integridad y disponibilidad de información que resida o se transmita por medios tecnológicos

4.5.2.2. Comité de Administración Integral de Riesgos

El Comité de Administración Integral de Riesgos (CAIR) de la Corporación Financiera Nacional, es responsable entre otros aspectos de[51]:

- Evaluar las políticas de seguridad de la información y someterlas a aprobación del Directorio

---

[50] Política de Seguridad de la Información, página 4.

[51] Ídem

- Proponer al Directorio modificaciones a la política de seguridad
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes
- Tomar conocimiento y supervisar la investigación de incidentes relativos a la seguridad
- Recomendar la aplicación de las principales iniciativas, estrategias y metodologías para incrementar la seguridad de la información

4.5.3. INTEGRACIÓN CON OTRAS ÁREAS

La coordinación y trabajo en equipo con las diferentes áreas que se mencionan a continuación, constituye un factor crítico de éxito en la implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información[52]

4.5.3.1. Gerencia General

Para la aprobación de normas y procedimientos de seguridad de la información, la designación de propietarios de la información, asignación de roles y responsabilidades, y la coordinación de iniciativas que requieran la colaboración de diferentes áreas de la institución

4.5.3.2. Gerencia Nacional de Riesgos

Para una gestión integral de los riesgos corporativos.

4.5.3.3. Gerencia de División de Informática

Para la implementación de sistemas, herramientas, controles tecnológicos y requerimientos de seguridad destinados a cumplir con la política, normas, estándares y procedimientos de seguridad de la información.

---

[52] Juan Matalobos, Análisis de Riesgos de Seguridad de la Información, página 169

4.5.3.4. Gerencia Administrativa

Para la implementación de la política, normas y estándares de seguridad relacionados a la seguridad física y ambiental.

4.5.3.5. Gerencia de Recursos Humanos

Para notificar a todo el personal que ingresa a prestar sus servicios profesionales en institución cualquiera sea su modo de vinculación, sobre sus obligaciones respecto del cumplimiento de la política de seguridad de la información y todas las normas, procedimientos y prácticas que de ellas surjan.

De igual manera, para difundir a todo el personal, los cambios que se produzcan respecto de la política, normas y procedimientos operativos de seguridad.

Para la suscripción de los Acuerdos de Confidencialidad, y, las tareas de formación y concienciación continua en materia de seguridad en coordinación con el Área de Seguridad.

4.5.3.6. Asesoría Jurídica

Para verificar el cumplimiento de la política de seguridad en la gestión de los contratos, acuerdos u otra documentación legal de la institución suscrita con funcionarios o con terceros. Asimismo, para asesorar en materia legal a la entidad, en lo que se refiere a la seguridad de la información.

4.5.3.7. Auditoría Interna

Debido a la necesidad de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de

seguridad de la información establecidas en la política, normas, estándares y procedimientos.

4.6. ANÁLISIS Y VALIDACIÓN DE APLICABILIDAD DE LA PROPUESTA

4.6.1. REFERENTE A LA METODOLOGÍA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El análisis de riesgos se lo ha realizado partiendo de dos pilares fundamentales, como son el inventario de activos de información considerando su grado de sensitividad, y, los requerimientos o necesidades del negocio respecto a la seguridad de la información; seguidamente, identificando las vulnerabilidades y amenazas a fin de establecer el nivel de riesgo bruto y residual, finalmente, planteando las medidas de prevención o remediación.

Dada una primera aplicación exitosa del proceso, se ha evidenciado que la metodología de gestión de riesgos de seguridad de la información propuesta se ajusta a la realidad operativa y financiera de la Corporación Financiera Nacional.

El grado de validez de un análisis de riesgos depende de la medida en la que sus resultados son aplicables a la Institución; el considerar los requerimientos y necesidades del negocio ha sido crucial, puesto que ha permitido alinear de manera transparente la Seguridad de la Información con los objetivos y estrategias Institucionales.

Por otro lado, si el análisis de riesgos estuviera basado únicamente en aspectos tecnológicos, existiría la probabilidad de no satisfacer al negocio, pudiendo incluso entorpecer los esfuerzos Institucionales de implementar sus estrategias y lograr sus metas.

Otra forma de validar el análisis de riesgos que se llevó a cabo, consiste en realizar una selección de controles más relevantes y verificar que su grado de implantación y su eficacia cumplen con el objetivo de mitigar los riesgos identificados.

En función de los controles seleccionados se pueden realizar test de intrusión[53] con distintos enfoques:

- Pruebas de caja negra[54]: consiste en simular los métodos de ataque que un hacker ejecuta con sus propios recursos, éste sólo dispone de información pública sobre el objetivo, e intenta identificar los agujeros de seguridad que puedan comprometer información sensible o las operaciones del sistema.
- Pruebas de caja blanca[55]: En este tipo de pruebas, previo a su ejecución se provee toda la información necesaria para una evaluación más profunda y real de la seguridad, incluye código fuente, archivos de configuración, documentación, diagramas, etc. Una ventaja es que identifican no sólo las vulnerabilidades inmediatas, sino también secciones de código y configuraciones potencialmente peligrosas, puertas traseras, y defectos de construcción, sin embargo, requiere más tiempo y esfuerzo, por tanto demanda más recursos.
- Pruebas de caja gris[56]: combina las pruebas de caja negra y caja blanca, se ejecutan métodos similares a los de la caja negra simulando ataques reales, la diferencia es que el atacante que

[53] El objetivo del **Test de Intrusión** es evaluar el estado de los sistemas, equipos o redes frente a ataques maliciosos de tipo intrusivo – http://www.isecauditors.com/es/test-intrusion.html, consultado en septiembre de 2012.

[54] Comprobación de la seguridad de los sistemas con un Test de intrusión, http://www.a2secure.com/auditorias/test-de-intrusion, consultado en septiembre de 2012

[55] Ídem

[56] Ídem

dispone de información pública, está permitido solicitar información adicional; este tipo de prueba es muy efectivo para identificar el mayor número real de amenazas como sea posible en el menor tiempo disponible.

Complementariamente, la metodología de riesgos de seguridad de la información propuesta, se alinea perfectamente a los requerimientos de evaluación de riesgos exigidos en la norma ISO/IEC 27001:2005, ya que contempla todas sus fases y se apoya en aspectos relevantes de Seguridad que corresponden a los dominios, objetivos de control y controles del Anexo A de la referida norma internacional.

4.6.2. REFERENTE AL MODELO DE SEGURIDAD DE LA INFORMACIÓN

El modelo de Gestión de Seguridad de la Información planteado, parte de los resultados obtenidos en el proceso de gestión de riesgos realizado, y constituye un proceso mas no un proyecto, por tanto, goza de las siguientes características:

- Continuo: tiene un principio y no un fin
- Mejorable: aplica el enfoque de mejora continua PDCA por procesos
- Entrada: tiene como principal insumo el resultado de la gestión de riesgos, que tiene una aplicabilidad en CFN analizada y validada
- Salida: seguridad de la información gestionada, basada en los requerimientos y necesidades del negocio, por tanto alineada a los objetivos institucionales

La implementación del Modelo de Gestión de Seguridad de la Información propuesto para la Corporación Financiera Nacional permitiría entre otras cosas:

- Contar con el apoyo de las autoridades para implementar las iniciativas en materia de seguridad de la información

- Obtener los recursos financieros, tecnológicos y humanos necesarios para su implementación, operación y mejora
- Mantener un orden en la gestión de seguridad de la información
- Asegurar que no quedan aspectos sueltos sin considerar o gestionar
- Dar un seguimiento formal a la gestión de seguridad
- Garantizar que la gestión de seguridad incluye la adopción de medidas preventivas y correctivas que lleven a reducir el impacto de posibles incidentes
- Dar visibilidad a la gestión de seguridad que se lleva a cabo
- Generar mejoras tanto en los procesos de negocio como en los procesos de seguridad y tecnológicos
- Formar y concienciar a los funcionarios de CFN

Al proponer un Modelo de Gestión de Seguridad basado en ISO/IEC 27001:2005, se aprovecharía la realidad de la Corporación Financiera Nacional que cuenta con certificación ISO 9001:2000, que lo hace muy aplicable en CFN puesto que:

- Viabilizaría una futura certificación en materia de seguridad de la información
- Aseguraría una implementación integrada y consistente con los procesos y procedimientos existentes en CFN
- Delegaría el control de documentación y gestión de auditorías internas al área de Gestión de Calidad ISO de CFN
- Reutilizaría los procedimientos y mecanismos de control del Sistema de Gestión de Calidad ISO de CFN
- Permitiría centrarse directamente en la gestión propia de Seguridad de la Información

La realidad a la fecha de ejecución del análisis y evaluación de riesgos de seguridad de la información en CFN es que no cuenta con un sistema de gestión de seguridad de la información, y a pesar de que se han realizado

importantes esfuerzos en esta materia, sus resultados son esfuerzos aislados y de cierta forma desordenados, si evaluamos esta situación con el Modelo de Madurez de Cobit (CMM), la gestión de seguridad se encuentra en un nivel de madurez entre 1 – Inicial y 2 - Repetible, con el modelo propuesto se espera llegar a un nivel 4 – Administrado.

Figura No 4.3: Modelo de madurez de Cobit

Representación gráfica de los modelos de madurez

Fuente: *Cobit*
Elaborado por: *Tania Guevara H.*

Tabla No 4.6: Impacto modelo de Gestión de Seguridad de la Información

	Ponderación actual MMC 0 - 5	Ponderación actual % MMC	Ponderación esperada MMC 0 - 5	Ponderación Esperada % MMC
Gestión de Seguridad de la Información	1.5	30.00	4	80.00

Elaborado por: *Tania Guevara H.*

4.6.3. EVIDENCIA DE APLICABILIDAD

Complementario a lo expresado en los puntos 4.6.1 y 4.6.2, es importante indicar que la propuesta realizada en el presente trabajo está siendo aplicada exitosamente en la CFN, a continuación se encuentra el detalle de los avances logrados en materia de seguridad de la información en relación a la implementación del plan de Seguridad (fruto de la aplicación de la metodología de riesgos desarrollada), y, del modelo de gestión seguridad de la información propuesto.

Tabla No 4.7: Seguimiento de Implementación del Plan de Seguridad

Plan de Seguridad de Información	**Corte Junio/2013**		
	Implementación	**% Cump**	**Objetivo cumplido (a cumplirse)**
Proy1 - Fortalecimiento de Normativa de Seguridad Institucional y documentación relacionada			
P1 - Generar la normativa complementaria conforme la norma ISO/IEC 27.001	Actualización de la política, normas y estándares conforme nuevos requerimientos: Control de Accesos Gestión de Activos Adq, Desarr y Manten, de Sistemas Elaboración, aprobación normas y estándares de: Gestión Comunic. y Oper Gestión Incidentes	55%	Conforme el alcance del trabajo realizado se ha cumplido el objetivo de normar y estandarizar la gestión de Comunicaciones y Operaciones, lo cual constituye una guía y orientación para el desarrollo e implementación de controles sobre los sistemas de información y relacionados permitiendo una mayor madurez respecto a seguridad de información (crecimiento ordenado). Se establece como avance global un 55 % debido a que la ISO/IEC 27001 consta de 11 dominios en total
P1 - Incluir aspectos de seguridad en procesos relacionados (tecnológicos)	La Gerencia de División de Informática GDI, ha elaborado/actualizado sus procedimientos considerando la participación activa y obligatoria del personal de Seguridad Informática	100%	Garantiza la inclusión de aspectos de seguridad en las primeras instancias de un proyecto o iniciativa tecnológica minimizando a futuro costos de mantenimiento o de ajustes.
Proy2 - Fortalecimiento Plan de Concienciación de Seguridad de la Información			
P4, P5, O1, O2, O3, P10 - Continuar y profundizar la ejecución del Plan de Concienciación	Desde el 2011 hasta la presente fecha se han desplegado: 12 boletines informativos 1 capacitación mediante Aula Virtual con evaluación 2 charlas formales para usuario final a todo el personal 2 charlas formales técnicas al personal de la GDI y auditoría informática 10 charlas de inducción /(personal nuevo)	100%	Se ha mantenido operativo el programa de concienciación Compromiso de la alta gerencia respecto a seguridad Mayor nivel de compromiso institucional con la seguridad
Proy3 - Implantación de controles funcionales y tecnológicos			
SP3.1 - Seguridad vinculada al Recurso Humano			

P2 - Complementar el proceso de selección de personal con investigación de antecedentes (cargos críticos)	Este proyecto ha sido desplazado hasta que la nueva estructura institucional esté aprobada por el Ministerio de Relaciones Laborales	0%	
P3 - Realizar un plan de reemplazos (personal alterno) para cargos críticos	Este proyecto ha sido desplazado hasta que la nueva estructura institucional esté aprobada por el Ministerio de Relaciones Laborales	0%	
P23 - Revisar/complementar las funciones de auditoría informática	El fortalecimiento del área de Auditoría Informática depende de la Contraloría General del Estado, se encuentra contemplada dentro de su planificación para el presente año	20%	Evaluaciones de seguridad independientes y objetivas
SP3.2 - Seguridad para la Red			
P6 - Segmentar la Red	CFN incorporó la infraestructura necesaria para segmentar la red (switches) y se encuentra en proceso de culminar su configuración	70%	Resguardo de los servicios tecnológicos
P21 - Implementar una solución NAC	CFN adquirió e implementó una solución NAC basada en appliance	80%	Mantiene controlado el acceso a la infraestructura tecnológica y a los servicios que se prestan, adicional se minimiza la posibilidad de que se materialicen amenazas frente a posibles vulnerabilidades que existan
P7 - Cifrar información confidencial tanto en almacenamiento como en tránsito	Canales de comunicaciones se encuentran cifradas, se adquirió una solución para la encriptación de información de estaciones de trabajo, está en proceso su implementación	50%	Garantiza la confidencialidad de la información
SP3.3 - Seguridad en ambientes tecnológicos - Producción			
Automatizar (implementar herramientas) para:			
P8 - Garantizar administración remota de forma segura	CFN adquirió e implementó una solución para VPN basada en appliance combinado con otra solución para autenticación robusta (doble factor de autenticación) con el fin de cubrir la administración remota de la infraestructura Se está trabajando en la red interna (complemento de segmentación y NAC)	60%	Administración remota segura para servidores y equipos de la infraestructura tecnológica.
P9 - Proceso de actualización de parches	Se implementó una solución para distribución de actualizaciones y parches de seguridad, se encuentra en proceso de fortalecimiento	70%	Equipos actualizados
P10 - Cifrar archivos críticos en estaciones de trabajo y servidores	CFN adquirió una solución para la encriptación de información de estaciones de trabajo, está en proceso su implementación	50%	Garantiza la confidencialidad de la información
O3 - Respaldo automatizado de información crítica en estaciones de trabajo	Proyecto planificado para el 2014	0%	
P11 - Complementar la documentación de tecnología y garantizar su aplicación	La GDI culminó el proceso de elaboración de documentación faltante de la mano con una firma consultora, proyecto auspiciado por el área de Desarrollo Organizacional debido a que CFN cuenta con certificación ISO9000	100%	Documentación que guía la actividad tecnológica y los servicios que la GDI brinda
P12 - Establecer Acuerdos de Nivel de Servicios tecnológicos	Este proyecto no ha sido posible emprenderlo debido a la priorización de otras actividades	0%	

P21 - Limitar la administración de equipos tecnológicos a PC's definidas	Se fortaleció la herramienta que permite la administración de PC's y se limitó a usuarios definidos	100%	Administración segura de Pc's
P24 - Evaluar mecanismos efectivos para control de consultas de información confidencial	Se ha solicitado la implementación de seguridad en el aplicativo Informes Cobis, el requerimiento debe ser priorizado	20%	Garantiza la confidencialidad de la información Cumplimiento de política, normas y estándares de seguridad Cumplimiento de regulaciones de organismos de control SBS
SP3.4 - Fortalecimiento del Sistema Identity Manager IDM			
P19 - Estandarizar la autenticación en las aplicaciones core del negocio	Proyecto planificado para el 2014	0%	
O4 - Integrar aplicaciones y estandarizar funcionalidad	Proyecto planificado para el 2014	0%	
Proy4 - Revisión de cumplimiento			
SP4.1 - Revisión y monitoreo en sistemas informáticos para actividades críticas de negocio			
P13 - Elaborar procedimientos para revisión y monitoreo regular	Los procedimientos para la revisión y monitoreo de log's han sido elaborados considerando las condiciones actuales de CFN	100%	Documentar las actividades regulares del área
P14 - Implementar pistas de auditoría integrales	Se ha solicitado la implementación de pistas de auditoria en los aplicativos críticos (conforme Plan de Continuidad del Negocio), el requerimiento debe ser priorizado	20%	Garantiza la auditabilidad de transacciones Estandarización de eventos e información almacenada Seguimiento de problemas Seguimiento de incidentes
P15 - Implementar monitoreos y revisiones periódicas	Se encuentra incluida en la planificación operativa del área de Seguridad, se debe validar la frecuencia	100%	Seguimiento de problemas Seguimiento de incidentes
SP4.2 - Implementación de herramienta para monitoreo centralizado			
P16 - Garantizar la integridad y permanencia de pistas de auditoría y log's de seguridad	Se está fortaleciendo la infraestructura tecnológica (adquisición plataforma SIEM), el proyecto se encuentra en fase de configuración de la herramienta	10%	Garantiza la integridad de la información Seguimiento de problemas Seguimiento de incidentes
P17, P18 - Implementar alertas tempranas (aplicativos de negocio y herramientas tecnológicas)	Adquisición de plataforma SIEM (para la parte de herramientas informáticas, respecto de aplicativos de negocio se incluyó en el P14)	10%	Seguimiento de problemas Seguimiento de incidentes
SP4.3 - Revisión y monitoreo (personal crítico, usuarios privilegiados, eventos críticos)			
P20 - Normar lineamientos para administración de claves sensibles, revisar su cumplimiento	Se encuentra normado	100%	Guía y soporte para la operación
P15 - Implementar monitoreos y revisiones periódicas	Se incrementará la frecuencia de revisión y monitoreo de log's con la finalización de implementación de la herramienta SIEM	10%	Seguimiento de problemas Seguimiento de incidentes
P22 - Auditar periódicamente las actividades de proveedores	Se adquirió una solución para control de accesos de cuentas privilegiadas, se encuentra en proceso de afinamiento de la herramienta	80%	Garantiza la auditabilidad de operaciones

Elaborado por: *Tania Guevara H.*

Tabla No 4.8: Implementación del modelo de gestión de seguridad de la información

	Corte junio/2013	
Modelo de Seguridad de la Información	**Implementación**	**% cumplimiento**
Cuerpo Normativo	Se cuenta con la siguiente documentación elaborada y aprobada por las instancias correspondientes: Política de seguridad Metodología de riesgos Plan de seguridad Procesos, procedimientos y registros Operativos Declaración de aplicabilidad Pendiente la aprobación explicita del alcance	83%
Responsabilidades de la dirección	Existe el comprimo explícito de la alta gerencia con la seguridad de la información El programa de formación y concienciación está vigente y operativo Se debe realizar revisiones independientes (al modelo en sí)	66%
Ejecución de procesos y controles	El plan de seguridad se encuentra en proceso de ejecución, lo cual, deriva en la implementación de controles. Pendiente la planificación y ejecución de auditorías y mejora del modelo de seguridad	50%
Clasificación de activos	Se cuenta con la documentación y procedimientos establecidos, adicional se está reportando a los organismos de control conforme la LOTAIP	100%
Gestión de riesgos	Se cuenta con la metodología para el análisis y evaluación de riesgos de seguridad para CFN	100%
Continuidad del negocio	Todas las acciones realizadas y planificadas contribuyen a apoyar la continuidad del negocio, adicional, se participa en las pruebas de dicho plan	66%

Elaborado por: *Tania Guevara H.*

Conforme se indicó en el punto 4.6.1, tercer párrafo "*El grado de validez de un análisis de riesgos depende de la medida en la que sus resultados son aplicables a la Institución…*", la tabla 4.7 pone de manifiesto la aplicabilidad de la metodología de riesgos de seguridad de la información, lo cual corrobora lo expresado en el mismo punto 4.6.1, segundo párrafo "*Dada una primera aplicación exitosa del proceso, se ha evidenciado que la metodología de gestión de riesgos de seguridad de la información propuesta se ajusta a la realidad operativa y financiera de la Corporación Financiera Nacional*"

Por otra parte la tabla 4.8 demuestra cómo el modelo de seguridad de la información propuesto está siendo implementado exitosamente en la CFN, hecho que se evidencia en sus porcentajes de avance.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Las principales conclusiones obtenidas durante el desarrollo del presente trabajo de tesis respecto han sido:

- Se ha logrado aplicar exitosamente el primer proceso de la metodología de gestión de riesgos de seguridad de la información propuesta para la Corporación Financiera Nacional
- Es fundamental conocer directamente las necesidades y requerimientos de seguridad del negocio, a fin de alinearlos a la gestión de seguridad de la información, lo que permite apoyar directamente a la consecución de las metas y estrategias Institucionales
- El apoyo y compromiso de la Dirección es indispensable para el desarrollo exitoso de las iniciativas de seguridad de la información, puesto que es el órgano rector para la provisión de recursos financieros y humanos, aprueba y respalda la ejecución de los planes o proyectos a implantar; y, motiva la colaboración de los diferentes funcionarios clave en los procesos requeridos
- Que la Corporación Financiera Nacional cuente con certificación ISO 9001, ha ayudado significativamente en el relevamiento de documentación y validación de procedimientos, complementariamente, este hecho facilita la implantación del modelo de gestión de seguridad propuesto
- Resulta indispensable respetar el alcance definido tanto para la Evaluación de Riesgos como para la aplicación del Sistema de Gestión de Seguridad de la Información, esto con el fin no extender interminablemente los trabajos, desviar la atención del objetivo primordial, y de viabilizar la aplicación de las medidas de tratamiento de los riesgos en el primer caso y de implantación del proceso de seguridad de la información para el segundo caso

- En el proceso de levantamiento de información - entrevistas debe ser llevado a cabo cuidadosamente, es importante la habilidad de comunicación del entrevistador para obtener toda la información necesaria de los entrevistados de forma imparcial y objetiva.
- Es necesario disponer de un conocimiento bastante aceptable tanto de tecnología como de seguridad de la información (productos y tendencias de mercado) para poder hacer recomendaciones aplicables y ajustadas a la realidad Institucional sobre los proyectos a emprender
- El eslabón más débil en la cadena de custodia y controles de la seguridad de la información es el recurso humanos, de ahí la importancia de mantener un programa de concienciación y formación que sea dinámico, creativo y constante
- Los controles a implementar no deben basarse únicamente en la tecnología[57], también se pueden y deben aplicar controles administrativos[58] y físicos[59]
- La implantación de un proceso formal de gestión de seguridad de la información aporta indirectamente en la mejora de los procesos de negocio ya que en cierta forma garantiza una consecución de objetivos ordenada, reduce reprocesos, facilita el control, entre otros
- Una certificación en materia de seguridad de la información, aporta los siguientes beneficios clave:

---

[57] Controles técnicos están relacionados con el acceso lógico, accesos de control, contraseñas, administración de recursos, métodos de identificación o autorización, seguridad de dispositivos y configuraciones de red, http://okay.com.mx/seguridad-de-la-informacion/los-tipos-de-controles-de-seguridad, consultado en septiembre de 2012.

[58] Controles administrativos son aquellos que están involucrados directamente con procedimientos, políticas, estándares, entrenamiento, procedimientos de monitoreo y control de cambios, http://okay.com.mx/seguridad-de-la-informacion/los-tipos-de-controles-de-seguridad, consultado en septiembre de 2012.

[59] Controles físicos están relacionados directamente con candados, monitores ambientales, guardias, perros entrenados, etc., http://okay.com.mx/seguridad-de-la-informacion/los-tipos-de-controles-de-seguridad, consultado en septiembre de 2012.

  - Garantiza el tratamiento y seguimiento formal de los incidentes de seguridad, por tanto la reducción en el impacto de los mismos que se traduce finalmente en reducción de costos
  - Confianza para clientes y partes interesadas (gerencia, socios, accionistas), gobierno para el caso de la CFN
  - Demostrable cumplimiento con los requisitos de los órganos de control
  - Ventaja competitiva
- Una institución certificada no implica que no tiene riesgos de seguridad de información, sino que tiene un adecuado sistema de gestión de dichos riesgos y proceso de mejora continua[60]
- Se evidenció que el modelo de Gestión de Seguridad de la Información propuesto es aplicable a CFN puesto que se lo está implementado en forma efectiva

[60] Seguridad de la Información, http://www.slideshare.net/disalazar/certificacion-iso-27001-isecsegurity-presentation, consultado en septiembre de 2012.

5.2. RECOMENDACIONES

Para concluir el presente trabajo de tesis me permito incluir las siguientes recomendaciones:

- Llevar a cabo procesos periódicos de análisis y evaluación de riesgos de seguridad de la información conforme la metodología propuesta
- Ampliar el alcance del análisis y evaluación de riesgos de seguridad de la información en los siguientes procesos
- Automatizar la gestión de riesgos propuesta
- Para futuros procesos y conforme la madurez de las evaluaciones de riesgos, pasar de una evaluación cualitativa a cuantitativa
- Complementar la documentación relacionada principalmente con elaboración de normas y estándares correspondientes a los 11 dominios de la norma ISO/IEC 17799:2000 – Tecnología de Información. Código de Prácticas para la Gestión de Seguridad de la Información.
- Continuar y fortalecer la ejecución del programa de formación y concienciación de seguridad de la información
- Realizar auditorías preventivas para mejorar la calidad de la gestión de seguridad de la información
- Invertir en seguridad preventiva, no en correctiva
- Fortalecer el recurso humano de las áreas técnicas, tanto de Seguridad Informática como de Tecnología de la Información
- Continuar la implantación del Modelo de Gestión de Seguridad de la Información propuesto en el presente trabajo de tesis hasta su culminación
- Obtener la certificación ISO/IEC 27001:2005

BIBLIOGRAFÍA

1. Ministerio de Administración Pública. *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Ver 2, I – Método*. España, 2006
2. Ministerio de Administración Pública. *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Ver 2. II – Catálogo de Elementos*. España, 2006
3. Ministerio de Administración Pública. *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Ver 2. III – Guía de Técnicas*. España, 2006
4. Instituto Ecuatoriano de Normalización, *NTEISO/IEC 27005 – Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información*. Ecuador, 2010
5. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Gestión de Riesgos Corporativos – Marco Integrado*. Estados Unidos, 2005
6. Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Gestión de Riesgos Corporativos – Marco Integrado – Técnicas de Aplicación*. Estados Unidos, 2005
7. Standards Association of Australia. *AS/NZS 4360:1999 Administración de Riesgos*. Australia, 1999
8. Asociación Española de Normalización y Certificación. *UNE-ISO/IEC 27001 Tecnología de Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información (SGSI)*. España, 2007
9. Isaca. *Cobit Control Objetives for Information and related Technology* Ver. 4.1
10. Juan Matalobos. *Análisis de Riesgos de Seguridad de la Información*. España, 2009
11. Política de Seguridad de la Información de la CFN, 2011
12. Normas y Estándares de la Gestión de Activos de la CFN, 2011
13. SI-26 Procedimiento para la Clasificación de la Información de la CFN, 2011

14. Programa de Formación y Concienciación de Seguridad de la Información de la CFN, 2011-2012
15. Instituto Ecuatoriano de Normalización, http://www.inen.gob.ec/index.php?option=com_content&view=article&id=206&Itemid=62, consultado en agosto del 2012
16. A2SECURE. http://www.a2secure.com/auditorias/test-de-intrusion, consultado en septiembre de 2012
17. AXELERATUM. http://axeleratum.com/2012/icomo-hacer-un-plan-de-trabajo-establecimiento-de-metricas/#, consultado en septiembre de 2012
18. Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento. http://www.agesic.gub.uy/innovaportal/file/1217/1/politica_de_gestion_de_incidentes.pdf, consultado en septiembre de 2012
19. Internet Security Auditors. http://www.isecauditors.com/es/test-intrusion.html, consultado en septiembre de 2012
20. http://okay.com.mx/seguridad-de-la-informacion/los-tipos-de-controles-de-seguridad, consulado en septiembre de 2012
21. ISEC Information Security Inc. http://www.slideshare.net/disalazar/certificacion-iso-27001-isecsegurity-presentation, consultado septiembre de 2012

ANEXOS

ANEXO A – REGISTRO DE LEVANTAMIENTO DE INFORMACIÓN

CONFIDENCIAL	
Registro de Levantamiento de Información **Gestión de Riesgos de Seguridad de la Información**	
Fecha:	
1. Datos personales	
Nombre:	
Cargo:	
Área:	
2. Relevamiento de Información	
2.1 Descripción general del proceso, área o producto	
2.2 Aspectos relevantes de Seguridad de la Información	
2.2.1. Política de Seguridad (Se relevará información respecto a la existencia y conocimiento de la política y normativa de seguridad)	
2.2.2. Aspectos Organizativos de la Seguridad de la Información (Se relaciona con la estructura organizacional de Seguridad, comité al que reporta, funciones y responsabilidades, acuerdos de confidencialidad, terceros, etc.)	
2.2.3. Gestión de Activos (Relacionado con el inventario, clasificación, etiquetado y manipulación de activos, propietarios de la información, etc.)	
2.2.4. Seguridad Ligada a los Recursos Humanos (Referente a procesos ejecutados antes, durante y después del empleo,	

concienciación, etc.)
2.2.5. Seguridad Física y Ambiental (Relativo a la seguridad de áreas físicas, accesos, centro de cómputo, etc.)
2.2.6. Gestión de Comunicaciones y Operaciones (Relacionado con responsabilidades y procedimientos de operación sean internos o provistos por terceros, gestión de capacidad, antivirus, código malicioso, respaldos, seguridad de red, correo electrónico, comercio electrónico, pistas de auditoría, alertas, entre otros)
2.2.7. Control de Accesos (Relacionado con identificación, autenticación, autorización de usuarios, controles de acceso a la red, sistemas operativos, responsabilidades del usuario, etc.)
2.2.8. Adquisición, mantenimiento y desarrollo de los sistemas de información (Referente a la seguridad implementada en los aplicativos informáticos – integridad, controles criptográficos, ambientes de procesamiento, entre otros)
2.2.9. Gestión de Incidentes de Seguridad (Relacionado con los procedimientos y gestión de notificaciones de eventos de seguridad)
2.2.10. Gestión de Continuidad del negocio (Vinculado con planes de continuidad del negocio, recuperación de desastres, planes de contingencia, etc.)
2.2.11. Cumplimiento (Relacionado con el cumplimiento de requisitos legales y reglamentarios de la CFN y de organismos de control, entre otros)
2.3. Expectativas / Sugerencias

Los aspectos relevantes de Seguridad que se han considerado para el presente trabajo de tesis son los once dominios de Seguridad de la Información propuestos en el Anexo A de la Norma ISO/IEC 27001:2005 – Sistema de Gestión de Seguridad de la Información (SGSI) – Requisitos.

ANEXO B – CATÁLOGO DE AMENAZAS

	Afectación a propiedades de Seguridad de la Información		
Amenaza	**Confidencialidad**	**Integridad**	**Disponibilidad**
Abuso de privilegios de acceso	x	x	
Acceso no autorizado	x	x	
Alteración de información		x	
Análisis de tráfico	x		
Caída del sistema			X
Condiciones inadecuadas de temperatura y/o humedad			X
Daño a la integridad de la información		x	
Daño a la integridad del sistema		x	
Daño físico de equipos			X
Daños por agua			X
Denegación de servicio			X
Desastres naturales (climáticos, sísmicos, volcánicos)			X
Destrucción de información			X
Difusión de software dañino	x	x	X
Divulgación de información	x		
Errores de los usuarios	x	x	X
Errores de mantenimiento / actualización de equipos (hardware)			X
Errores del administrador / configuración	x	x	X
Espionaje industrial	x		
Falsificación de privilegios	x	x	
Fraude	x	x	
Fuego			X
Fuga de información	x		
Genera brechas de seguridad	x	x	X
Genera incidentes de seguridad	x	x	X
Indisponibilidad del personal			X
Ingeniería social	x	x	
Interceptación de información	x		
Manipulación de la configuración	x	x	X
Manipulación de programas	x	x	
Pérdida de servicios esenciales (energía, agua, telecomunicaciones)			X
Robo/Pérdida de información	x		X
Suplantación de identidad	x	x	

ANEXO C - CRITERIOS PARA CALIFICAR LA PROBABILIDAD DE OCURRENCIA

Probabilidad de Ocurrencia	Descripción
Muy Alta	• Mayor a 2 incidentes de seguridad por año generando pérdida financiera • Se espera la ocurrencia del evento en el 80% de los casos • Casi con certeza se espera la ocurrencia del evento • El mismo evento ocurrirá con cierta periodicidad (1 vez cada mes)
Alta	• Un incidente de seguridad por año generando pérdida financiera • El evento ocurrirá entre el 60 y el 80% de los casos • Significativa probabilidad de ocurrencia • Se presenta con alguna frecuencia (1 vez cada trimestre)
Moderada	• 1 incidente de seguridad por año • El evento puede ocurrir entre el 40 y 60% de los casos • Mediana probabilidad de ocurrencia
Baja	• No se ha presentado incidentes de seguridad. • El evento puede ocurrir entre el 20 y el 40% de los casos • Baja probabilidad de ocurrencia • Se ha presentado alguna vez en la CFN
Muy Baja	• El evento puede ocurrir entre el 5 al 20% de los casos • Muy baja probabilidad de ocurrencia • Nunca ha ocurrido

ANEXO D - CRITERIOS PARA CALIFICAR EL NIVEL DE IMPACTO

Nivel de Impacto	Descripción
Catastrófico	• Interrupción total de la operación de la CFN. • Pérdida de información del negocio clasificada como confidencial de la CFN o de terceros que no se puede recuperar
Mayor	• Daño competitivo a la CFN (fuga de estrategia de un nuevo producto que provoque reducción de clientes, fuga información genera pérdida financiera, etc.). • Incidentes que generan casos de violación o incumplimiento de la ley y política interna provocando observaciones o sanciones por parte de los Organismos de Control. • Imagen negativa de la CFN ante sus clientes debido a fraudes. • Pérdida de información del negocio de CFN o de terceros que sea recuperable • Daño en la integridad de la información clasificada como confidencial. • Daño de facilidades tecnológicas (centro de datos donde se almacene o transporte información clasificada como confidencial). • No disponer de los servicios de procesos del negocio. • No disponer de procedimientos críticos (manejan, transportan, almacenan información confidencial)
Moderado	• Interrupción de los procesos de apoyo. • Imagen negativa ante sus clientes por no estar disponible los servicios que presta la CFN a través de la página web. • Daño en la integridad de la información clasificada como de uso interno, pública o en las facilidades tecnológicas que

	transporten o almacenen dicha información. • Fuga de información confidencial de CFN que no genere pérdida financiera. • Reproceso de actividades negocio, con efecto de aumento de la carga operativa • Incumplimiento de los procedimientos internos de seguridad.
Menor	• Fuga de información clasificada de uso interno. • Infección de virus en software (computadores) de la Entidad. • Afectación de los niveles de servicio a clientes por incumplimiento en la entrega de información causado por indisponibilidad de servicios informáticos. • Reproceso de actividades de apoyo con efecto de aumento de la carga operativa.
Insignificante	• Prácticas improductivas/ fallas/ insuficiencias con respecto a la administración de la información que no contribuyen a la agilidad en el servicio al cliente.

ANEXO E – CRITERIOS PARA CALIFICAR EL RIESGO BRUTO

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
PROBABILIDAD	Muy Alta					
	Alta					
	Moderada					
	Baja					
	Muy Baja					

	RIESGO
	Superior
	Alto
	Moderado
	Bajo

ANEXO F – CRITERIOS PARA CALIFICAR LA EFICACIA DE CONTROLES

Eficacia	
Preventivo Automático Constante Si No	Fuerte
Preventivo Automático Por demanda Si No	Moderado
Preventivo Automático Diario Si No	Fuerte
Preventivo Automático Semanal Si No	Fuerte
Preventivo Automático Quincenal Si No	Fuerte
Preventivo Automático Mensual Si No	Fuerte
Preventivo Automático Trimestral Si No	Moderado
Preventivo Automático Cuatrimestral Si No	Moderado
Preventivo Automático Semestral Si No	Moderado
Preventivo Automático Anual Si No	Moderado
Preventivo Manual Constante Si No	Moderado
Preventivo Manual Por demanda Si No	Moderado
Preventivo Manual Diario Si No	Moderado
Preventivo Manual Semanal Si No	Moderado
Preventivo Manual Quincenal Si No	Moderado
Preventivo Manual Mensual Si No	Moderado
Preventivo Manual Trimestral Si No	Moderado
Preventivo Manual Cuatrimestral Si No	Moderado
Preventivo Manual Semestral Si No	Moderado
Preventivo Manual Anual Si No	Moderado
Detectivo Automático Constante Si No	Moderado
Detectivo Automático Por demanda Si No	Moderado
Detectivo Automático Diario Si No	Moderado
Detectivo Automático Semanal Si No	Moderado
Detectivo Automático Quincenal Si No	Moderado
Detectivo Automático Mensual Si No	Moderado
Detectivo Automático Trimestral Si No	Moderado
Detectivo Automático Cuatrimestral Si No	Moderado
Detectivo Automático Semestral Si No	Moderado
Detectivo Automático Anual Si No	Moderado
Detectivo Manual Constante Si No	Débil
Detectivo Manual Por demanda Si No	Débil
Detectivo Manual Diario Si No	Débil
Detectivo Manual Semanal Si No	Débil
Detectivo Manual Quincenal Si No	Débil
Detectivo Manual Mensual Si No	Débil
Detectivo Manual Trimestral Si No	Débil

Detectivo Manual Cuatrimestral Si No	Débil
Detectivo Manual Semestral Si No	Débil
Detectivo Manual Anual Si No	Débil
Preventivo Automático Constante No Si	Débil
Preventivo Automático Por demanda No Si	Débil
Preventivo Automático Diario No Si	Débil
Preventivo Automático Semanal No Si	Débil
Preventivo Automático Quincenal No Si	Débil
Preventivo Automático Mensual No Si	Débil
Preventivo Automático Trimestral No Si	Débil
Preventivo Automático Cuatrimestral No Si	Débil
Preventivo Automático Semestral No Si	Débil
Preventivo Automático Anual No Si	Débil
Preventivo Manual Constante No Si	Débil
Preventivo Manual Por demanda No Si	Débil
Preventivo Manual Diario No Si	Débil
Preventivo Manual Semanal No Si	Débil
Preventivo Manual Quincenal No Si	Débil
Preventivo Manual Mensual No Si	Débil
Preventivo Manual Trimestral No Si	Débil
Preventivo Manual Cuatrimestral No Si	Débil
Preventivo Manual Semestral No Si	Débil
Preventivo Manual Anual No Si	Débil
Detectivo Automático Constante No Si	Débil
Detectivo Automático Por demanda Si Si	Débil
Detectivo Automático Diario No Si	Débil
Detectivo Automático Semanal No Si	Débil
Detectivo Automático Quincenal No Si	Débil
Detectivo Automático Mensual No Si	Débil
Detectivo Automático Trimestral No Si	Débil
Detectivo Automático Cuatrimestral No Si	Débil
Detectivo Automático Semestral No Si	Débil
Detectivo Automático Anual No Si	Débil
Detectivo Manual Constante No Si	Débil
Detectivo Manual Por demanda No Si	Débil
Detectivo Manual Diario No Si	Débil
Detectivo Manual Semanal No Si	Débil
Detectivo Manual Quincenal No Si	Débil
Detectivo Manual Mensual No Si	Débil
Detectivo Manual Trimestral No Si	Débil
Detectivo Manual Cuatrimestral No Si	Débil
Detectivo Manual Semestral No Si	Débil

Detectivo Manual Anual No Si	Débil
Preventivo Automático Constante Si Si	Débil
Preventivo Automático Por demanda Si Si	Débil
Preventivo Automático Diario Si Si	Débil
Preventivo Automático Semanal Si Si	Débil
Preventivo Automático Quincenal Si Si	Débil
Preventivo Automático Mensual Si Si	Débil
Preventivo Automático Trimestral Si Si	Débil
Preventivo Automático Cuatrimestral Si Si	Débil
Preventivo Automático Semestral Si Si	Débil
Preventivo Automático Anual Si Si	Débil
Preventivo Manual Constante Si Si	Débil
Preventivo Manual Por demanda Si Si	Débil
Preventivo Manual Diario Si Si	Débil
Preventivo Manual Semanal Si Si	Débil
Preventivo Manual Quincenal Si Si	Débil
Preventivo Manual Mensual Si Si	Débil
Preventivo Manual Trimestral Si Si	Débil
Preventivo Manual Cuatrimestral Si Si	Débil
Preventivo Manual Semestral Si Si	Débil
Preventivo Manual Anual Si Si	Débil
Detectivo Automático Constante Si Si	Débil
Detectivo Automático Por demanda Si Si	Débil
Detectivo Automático Diario Si Si	Débil
Detectivo Automático Semanal Si Si	Débil
Detectivo Automático Quincenal Si Si	Débil
Detectivo Automático Mensual Si Si	Débil
Detectivo Automático Trimestral Si Si	Débil
Detectivo Automático Cuatrimestral Si Si	Débil
Detectivo Automático Semestral Si Si	Débil
Detectivo Automático Anual Si Si	Débil
Detectivo Manual Constante Si Si	Débil
Detectivo Manual Por demanda Si Si	Débil
Detectivo Manual Diario Si Si	Débil
Detectivo Manual Semanal Si Si	Débil
Detectivo Manual Quincenal Si Si	Débil
Detectivo Manual Mensual Si Si	Débil
Detectivo Manual Trimestral Si Si	Débil
Detectivo Manual Cuatrimestral Si Si	Débil
Detectivo Manual Semestral Si Si	Débil
Detectivo Manual Anual Si Si	Débil
Preventivo Automático Constante No No	Débil

Preventivo Automático Por demanda No No	Débil
Preventivo Automático Diario No No	Débil
Preventivo Automático Semanal No No	Débil
Preventivo Automático Quincenal No No	Débil
Preventivo Automático Mensual No No	Débil
Preventivo Automático Trimestral No No	Débil
Preventivo Automático Cuatrimestral No No	Débil
Preventivo Automático Semestral No No	Débil
Preventivo Automático Anual No No	Débil
Preventivo Manual Constante No No	Débil
Preventivo Manual Por demanda No No	Débil
Preventivo Manual Diario No No	Débil
Preventivo Manual Semanal No No	Débil
Preventivo Manual Quincenal No No	Débil
Preventivo Manual Mensual No No	Débil
Preventivo Manual Trimestral No No	Débil
Preventivo Manual Cuatrimestral No No	Débil
Preventivo Manual Semestral No No	Débil
Preventivo Manual Anual No No	Débil
Detectivo Automático Constante No No	Débil
Detectivo Automático Por demanda No No	Débil
Detectivo Automático Diario No No	Débil
Detectivo Automático Semanal No No	Débil
Detectivo Automático Quincenal No No	Débil
Detectivo Automático Mensual No No	Débil
Detectivo Automático Trimestral No No	Débil
Detectivo Automático Cuatrimestral No No	Débil
Detectivo Automático Semestral No No	Débil
Detectivo Automático Anual No No	Débil
Detectivo Manual Constante No No	Débil
Detectivo Manual Por demanda No No	Débil
Detectivo Manual Diario No No	Débil
Detectivo Manual Semanal No No	Débil
Detectivo Manual Quincenal No No	Débil
Detectivo Manual Mensual No No	Débil
Detectivo Manual Trimestral No No	Débil
Detectivo Manual Cuatrimestral No No	Débil
Detectivo Manual Semestral No No	Débil
Detectivo Manual Anual No No	Débil

ANEXO G – CRITERIOS PARA CALIFICAR EL RIESGO RESIDUAL

		EFICACIA CONTROL		
		Fuerte	Moderado	Débil
RIESGO BRUTO	Superior			
	Alto			
	Moderado			
	Bajo			

	RIESGO
	Superior
	Alto
	Moderado
	Bajo

ANEXO H – PROGRAMA DE FORMACIÓN Y CONCIENCIACIÓN

DEPARTAMENTO NACIONAL DE SEGURIDAD INFORMÁTICA
PROGRAMA DE FORMACIÓN Y CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN

PLANIFICACION AÑO 2011 CON PROYECCION 2012

RESPONSABLES

- Gerencia Nacional de Riesgos
- Departamento Nacional de Seguridad Informática
- Subgerencia Nacional de Recursos Humanos y Desarrollo Organizacional

CONCEPTO GENERAL

El Programa de Concienciación de Seguridad de la Información forma parte integral de la planificación del Departamento Nacional de Seguridad Informática, y es una herramienta de apoyo importante e indispensable para mejorar el nivel de madurez respecto a la Seguridad de la Información en la Corporación Financiera Nacional.

1. PROGRAMA QUE APUNTA A LA ESTRATEGIA INSTITUCIONAL

TERCER EJE ESTRATÉGICO CFN:

Fortalecer los procesos de soporte del negocio

OBJETIVOS ESTRATEGICOS CFN:

Objetivo 3. Recurso Tecnológico: Implementar una plataforma tecnológica de punta para sustentar las necesidades de la institución, teniendo como prioridad el cumplimiento de los objetivos planteados en el Plan Institucional.

Objetivo 4. Procesos Institucionales: Evaluar, seguir y actualizar los procesos institucionales enmarcados en alta eficiencia de tiempo y recursos.

2. OBJETIVOS DEL PROGRAMA

- Comunicar a los funcionarios de CFN la importancia de proteger la información institucional y fomentar la adopción de una cultura de seguridad en la información en sus actividades diarias

- Lograr que los funcionarios de CFN magnifiquen la responsabilidad que tienen en la protección de la confidencialidad, integridad y disponibilidad de los activos de información

- Fomentar una cultura de seguridad que convierta a los funcionarios de CFN en la primera barrera de seguridad de la información, y que comprendan que la seguridad no es sólo competencia de los especialistas en seguridad.

- Formar y concienciación sobre el uso seguro y responsable de la tecnología

- Aportar a la cultura del país en este tema

3. IMPORTANCIA

La información es uno de los activos más importantes y sensibles para la operación de todo negocio, por lo que requiere ser protegida adecuadamente. La seguridad de la información tiene como finalidad última el apoyar a la continuidad del negocio, minimizar los riesgos y maximizar el retorno de las inversiones, de tal forma que apuntale a la consecución de los objetivos Institucionales.

Por lo anterior, se debe preservar de la confidencialidad, integridad y disponibilidad de la información, basados en tres pilares fundamentales como son documentación institucional, personal capacitado y consciente, y tecnología

controlada. Varios expertos y estudios realizados indican que el eslabón más débil de la cadena es el personal, es por este motivo, que es de vital importancia que exista un programa de concienciación sobre seguridad de la información.

4. ELEMENTOS DEL PROGRAMA

Políticas y normas de seguridad de la información: documentos habilitantes que establecen responsabilidades en materia de seguridad y dan los lineamientos necesarios para la protección de los activos de información.

Audiencia: es el personal al que está dirigido los esfuerzos de formación y concienciación referente a seguridad de la información. La audiencia puede ser organizada y agrupada considerando diferentes elementos como el nivel de conocimiento tecnológico, nivel jerárquico, nivel de acceso a la información, por tipo de sistema o por sensibilidad frente a la seguridad de la información.

Apoyo de la alta gerencia: dada la importancia que tiene el contar con un programa de Concienciación de Seguridad de la Información, existe el compromiso manifiesto de las máximas Autoridades, quienes proveerán de los recursos necesarios, conseguirán el compromiso de los funcionarios, permitirán agilizar los procesos, y facilitarán el seguimiento.

Mecanismos de comunicación: son las diferentes estrategias que se pueden adoptar en la ejecución de una campaña de concienciación.

5. ALCANCE

La Seguridad de la Información es un tema que involucra a toda la CFN, por tanto, debe ser tratada como algo integral, en este sentido, el programa de concienciación de Seguridad de la Información será a nivel nacional.

6. DIRIGIDO A:

Funcionarios y pasantes de CFN. Personas externas de así determinarlo la Alta Gerencia.

7. ESTRATEGIAS

El programa de formación y concienciación de Seguridad de la Información se enfocará a dotar al funcionario de los conocimientos necesarios para la aplicación práctica de los lineamientos y acciones a seguir, difundiendo información sobre los riesgos en el manejo de la información y la manera de prevenirlos, adopción de buenas prácticas en el uso de los recursos tecnológicos, persuasión a nuestros compañeros para que estén más conscientes de este tema, entre otras.

Para la consecución de los objetivos del programa de concienciación se podrán seleccionar las siguientes estrategias, sin excluir la posibilidad de acoger nuevas iniciativas en el desarrollo del programa:

Definición de tópicos, privilegiando la enseñanza de cómo proteger nuestra información, entregando valor agregado para el funcionario a fin de que sea aplicable en el entorno laboral, familiar y personal; para su difusión se utilizarán diferentes canales de comunicación con los que cuente la CFN:

- Conferencias
- Talleres presenciales
- Video conferencia
- Cursos electrónicos
- Aula Virtual
- Mensajes por la intranet
- Mensajes de correo electrónico
- Documentos de comunicación interna

Campañas de formación y concienciación difundiendo conceptos puntuales para el uso adecuado de los recursos tecnológicos:

- Comunicaciones por web
- Boletines informativos virtuales
- Notas en la cartelera de información
- Mensajes de correo electrónico
- Documentos de comunicación interna
- Artículos y publicaciones especializadas

Las diferentes estrategias no son exclusivas, por lo contrario, son complementarias y permanentes.

8. PLANIFICACIÓN

Planificación año 2011 - 2012, orientado a la continuidad.

PLANIFICACIÓN DE FORMACIÓN Y CONCIENCIACIÓN DE SEGURIDAD DE LA INFORMACIÓN - 2011 -2012													
Proyecto	**ACTIVIDADES**	**ENERO**	**FEBRERO**	**MARZO**	**ABRIL**	**MAYO**	**JUNIO**	**JULIO**	**AGOSTO**	**SEPTIEMBRE**	**OCTUBRE**	**NOVIEMBRE**	**DICIEMBRE**
Definición / Actualización Documentación	Definición y actualización de normas de Seguridad basadas en un Sistema de Gestión de Seguridad de la Información (SGSI)		x					x			x		
	Elaboración / Actualización de procedimientos de seguridad		X				x					x	
Formación y Concientización, análisis indicador	Inducción personal nuevo*	x	x	x	x	x	x	X	x	x	x	x	x
	Notificación formal a los propietarios de los activos de información, notificar sus responsabilidades.		x										
	Revisión uso Internet, análisis indicador			x				x				x	
	Campañas de concienciación, análisis indicador		x		x		x		x		x		x
	Visita Sucursales			x							x		
	Capacitación formal sobre seguridad informática						x	X					

Nota: el envío de mensajes por otros medios como correo electrónico, intranet se podrán enviar independientemente de la planificación
* Depende de Recursos Humanos en relación a los ingresos de personal

9. INDICADORES

Permitirán establecer la eficiencia del programa y aplicar los correctivos necesarios para su adecuado funcionamiento

Indicador	Descripción	Mide
Cubrimiento del programa de concienciación en seguridad	Porcentaje acumulado de Funcionarios a quienes se les ha dado entrenamiento en seguridad, a una fecha determinada, con relación al total funcionarios de CFN	El nivel de cubrimiento del programa
Uso de Internet	Nivel de uso adecuado del Internet (tipo de páginas visitadas, tiempo utilizado, bytes transmitidos)	Cómo el programa de concienciación, ha ayudado a la optimización del uso de Internet (reducción/aumento)

Elaborado: Xxxxx Xxxxxx		Aprobado: Xxxxx Xxxxxx
Jefe Nal de Seguridad Informática		Gerente Nacional de Riesgos

ANEXO I – DECLARACIÓN DE APLICABILIDAD

Objetivo de Control	Control	Aplica	Esta Implantado	Documento de referencia
		Si / No	Si / No / Parcial	
A.5 Política de Seguridad				
5.1 Política de Seguridad de la Información	5.1.1 Documentar Política de Seguridad de la Información	Si	Si	Política de Seguridad de la Información
	5.1.2 Revisión de la Política de Seguridad de la Información	Si	Si	Actualización de la Oolítica de Seguridad de la Información periódica
A.8 Seguridad Ligada al Recurso Humano				
A.8.1 Antes del Empleo	8.1.1 Funciones y Responsabilidades	Si	Parcial	Política de Seguridad de la Información Se debería incluir las funciones y responsabilidades en el orgánico funcional o en el perfil de los puestos
	8.1.2 Investigación de antecedentes	Si	Si	Proceso de selección de Recursos Humanos PRH-03 Flujograma Reclutar personal PRH-03 Instrucciones Reclutar personal Bases del concurso de méritos y oposición" (RPRH-05) RPRH-06 Convocatoria a concurso de méritos y oposición RPRH-10 Guía de entrevista
	8.1.3 Términos y Condiciones de la contratación	Si	Si	RPRH-11 Acción de Personal o contrato
A.8.2 Durante el Empleo	8.2.1 Responsabilidades de la dirección	Si	Si	Disposiciones de la Administración Contratos con terceros
	8.2.2 Concienciación, formación y capacitación en Seguridad de la Información	Si	Si	Programa de formación y concienciación en materia de seguridad de la información
	8.2.3 Proceso disciplinario	Si	Si	Política de Seguridad de la Información
A.8.3 Cese del empleo o cambio de puesto	8.3.1 Responsabilidades del cese o cambio	Si	Si	Proceso de desvinculación de Recursos Humanos RPRH-11 Acción de Personal o contrato
	8.3.2 Devolución de activos	Si	Si	RPBS-02 Acta de entrega recepción de bien
	8.3.3 Retirada de los derechos de acceso	Si	Si	RSI - Eliminación de cuentas

A.10 Gestión de Comunicaciones y Operaciones				
A.10.1 Responsabilidades y procedimientos de operación	10.1.1 Documentación de los procedimientos de operación	Si	No	Se debe documentar
	10.1.2 Gestión de Cambios	Si	Parcial	Proceso de control de cambios Se debe validar el proceso y actualizar/ complementar la documentación
	10.1.3 Segregación de tareas	Si	Parcial	Conforme el recurso humano disponible Se debe fortalecer el recurso humano
	10.1.4 Separación de los recursos de desarrollo y operación	Si	Parcial	Existe ambientes para producción, desarrollo y pruebas Se debe fortalecer los ambientes, segmentación de redes, firewalls, despersonalización de la información, etc.
A.10.2 Gestión de la provisión de servicios por terceros	10.2.1 Provisión de servicios	Si	Si	Revisión de cumplimiento del contrato previo a pago de facturas
	10.2.2 Supervisión y revisión de los servicios prestados por terceros	Si	Parcial	Verificación contra entregables Verificación de disponibilidad de servicios Se debe fortalecer con herramientas automatizadas
	10.2.3 Gestión de cambios en los servicios prestados por terceros	Si	Parcial	Gestión de cambios en aplicaciones de negocio provistos por terceros Se debe aplicar la gestión de cambios en todos los proyectos informáticos (software, hardware y comunicaciones)
A.10.3 Planeación y aceptación del sistema	10.3.1 Gestión de Capacidades	Si	Parcial	Gestión de capacidades en infraestructura (servidores y comunicaciones) Se debe gestionar formalmente la capacidad en todos los recursos tecnológicos
	10.3.2 Aceptación del sistema	Si	No	El proceso de calidad QA debe instaurarse en todos los proyectos tecnológicos
A.10.4 Protección contra código malicioso y descargable	10.4.1 Controles contra el código malicioso	Si	Parcial	Antivirus (LAN y perimetral) Se debe reformar la suite de seguridad de puntos finales
	10.4.2 Controles contra el código descargable en el cliente	Si	Parcial	Antivirus (LAN y perimetral) Se debe reformar la suite de seguridad de puntos finales
A.10.5 Copias de Seguridad	10.5.1 Copias de seguridad de la información	Si	Parcial	Se obtiene copias de seguridad Se debe validar periodicidad y complementar con restauraciones periódicas planificadas
A.10.6 Gestión de Seguridad de las redes	10.6.1 Controles de red	Si	No	Se debe implementar solución NAC, encriptación

	10.6.2 Seguridad de los servicios de red	Si	Parcial	Servicios de file system, impresión, DHCP, etc. Se debe implementar solución NAC, encriptación
A.10.7 Manipulación de los soportes	10.7.1 Gestión de soportes extraíbles	Si	Parcial	RPBS-02 Acta de entrega recepción de bien Se debe revisar el procedimiento y fortalecerlo
	10.7.2 Retirada de soportes	Si	Parcial	RPBS-02 Acta de entrega recepción de bien Se debe revisar el procedimiento y fortalecerlo
	10.7.3 Procedimientos de manipulación de la información	Si	No	Elaborar procedimientos
	10.7.4 Seguridad de la documentación del sistema	Si	No	Se debe documentar y mantener actualizada
A.10.8 Intercambio de Información	10.8.1 Políticas y procedimientos de intercambio de información	Si	Parcial	Política de Seguridad de la Información Elaborar normas y estándares
	10.8.2 Acuerdos de intercambio	Si	Parcial	Se incluyen como parte de la contratación de servicios o convenios con otras entidades
	10.8.3 Soportes físicos en tránsito	Si	No	Elaborar normativa
	10.8.4 Mensajería electrónica	Si	No	Implementar mecanismos para acceso seguro al correo protección de la información utilizando este medio
	10.8.5 Sistemas de información empresariales	Si	Si	Política de Seguridad de la Información Norma de Adquisición, Mantenimiento y Desarrollo de Sistemas de Información
A.10.9 Servicios de Comercio Electrónico	10.9.1 Comercio electrónico	No	No	La CFN no cuenta ni hace uso de este tipo de servicios
	10.9.2 Transacciones en línea	Si	Si	Seguridades propias de las entidades que prestan el servicio (Banco Central del Ecuador, Swift)
	10.9.3 Información puesta a disposición pública	Si	Si	Servicio contratado
A.10.10 Supervisión	10.10.1 Registro de Auditoría	Si	Parcial	Pistas de auditoría en aplicaciones Se debe validar la existencia y suficiencia de las pistas de auditoría, adicional se debe disponer de mecanismos para la visualización de esta información

	10.10.2 Supervisión del uso del sistema	Si	Parcial	Procedimiento para el monitoreo y revisión de log's Revisión de auditoría en servidores Novell Revisión de Log de Base de Datos Revisión de Log de servidores Linux Revisión de Pistas Seguridad PCIE Revisión de actividad de equipos de seguridad perimetral Revisión de uso adecuado de recursos Se debe fortalecer el proceso con herramientas que centralicen la administración, permitan emitir alarmas tempranas y dinamizar la periodicidad de revisión
	10.10.3 Protección de la información de los registros	Si	No	Implementar mecanismos para la protección de los registros de auditoria
	10.10.4 Registros de administración y operación	Si	No	Implementar un herramienta para el control y gestión de usuarios privilegiados
	10.10.5 Registro de fallos	Si	Parcial	Se debe implementar en todos los sistemas y herramientas tecnológicas
	10.10.6 Sincronización del Reloj	Si	No	Implementar sincronización del tiempo con una fuente externa confiable
A.11 Control de Accesos				
A.11.1 Requerimientos del negocio para el control de acceso	11.1.1 Política de control de acceso	Si	Si	Política de Seguridad de la Información Norma de Control de Accesos
A.11.2 Gestión de Acceso del Usuario	11.2.1 Registro de usuario	Si	Si	Procedimiento para crear cuentas en los diferentes sistemas de negocio y herramientas tecnológicas
	11.2.2 Gestión de privilegios	Si	Si	Mapa de Cargos/roles (perfiles) Procedimiento para administración de roles Procedimiento para depuración de cuentas Procedimiento para eliminación de cuentas
	11.2.3 Gestión de contraseñas de usuario	Si	Si	Procedimiento para reseteo claves y desbloqueo de cuentas de red
	11.2.4 Revisión de los derechos de acceso de usuario	Si	Si	RH-09 Procedimiento para realizar traslados, cambios administrativos. RH-11 Procedimiento para vacaciones, licencias, y permisos
A.11.3 Responsabilidades de usuario	11.3.1 Uso de contraseña	Si	Si	Política de Seguridad de la Información Programa de Formación y Concienciación Se debe reforzar en concienciación

	11.2.2 Equipo de usuario desatendido	Si	Si	Política de Seguridad de la Información Programa de Formación y Concienciación Política distribuida por zenwork Se debe reforzar en concienciación y validación del cumplimiento
	11.2.3 Política de puesto de trabajo despejado y pantalla limpia	Si	Parcial	Política de Seguridad de la Información Programa de Formación y Concienciación Se debe reforzar en concienciación y validación del cumplimiento
A.11.4 Control de acceso a la red	11.4.1 Política de uso de los servicios en red	Si	Si	Política de Seguridad de la Información Norma de control de accesos
	11.4.2 Autenticación de usuario para conexiones externas	Si	No	No existen ni se permiten conexiones remotas
	11.4.3 Identificación de los equipos en las redes	Si	No	Implementar control
	11.4.4 Diagnóstico remoto y protección de los puertos de configuración	Si	No	Implementar control
	11.4.5 Segregación de las redes	Si	No	Se debe segmentar la red
	11.4.6 Control de la conexión a la red	Si	Parcial	Se limitan los usuarios con privilegios para conectarse a redes externas Se debe reformar y validar
	11.4.7 Control de encaminamiento (routing) de red	Si	Parcial	Servicio contratado Se debe reforzar el control
A.11.5 Control de acceso al sistema operativo	11.5.1 Procedimientos seguros de inicio de sesión	Si	Parcial	Se tiene identificación y autenticación Se debe reforzar con soluciones tipo NAC
	11.5.2 Identificación y autenticación de usuario	Si	Si	Se tiene identificación y autenticación
	11.5.3 Sistema de gestión de contraseñas	Si	Parcial	Se gestiona la contraseña con varios parámetros Se debe unificar la contraseña para robustecerla
	11.5.4 Uso de los recursos del sistema	Si	No	Se debe implementar controles
	11.5.5 Desconexión automática de sesión	Si	Parcial	Solo algunos sistemas cuentan con esta característica Se debe implementar en todos los sistemas
	11.5.6 Limitación del tiempo de conexión	Si	Parcial	Solo algunos sistemas cuentan con esta característica Se debe implementar en todos los sistemas

A.11.6 Control de acceso a las aplicaciones y a la información	11.6.1 Restricción del acceso a la información	Si	Parcial	Se controla el acceso a la información en la mayoría de sistemas Se debe implementar seguridad en todas las aplicaciones de negocio
	11.6.2 Aislamiento de sistemas sensibles	Si	No	Se debe implementar conforme los requerimientos del negocio
A.11.7 Ordenadores portátiles y teletrabajo	11.7.1 Ordenadores portátiles y comunicaciones móviles	Si	Parcial	Política de Seguridad de la Información Se debe ampliar la política para considerar equipamiento móvil y aplicar controles
	11.7.2 Tele-trabajo	No	No	La CFN no cuenta ni hace uso de este tipo de servicio